

**PUBLIC APPENDIX—
SEALED MATERIAL IN SEPARATE SUPPLEMENT**
ORAL ARGUMENT SCHEDULED FOR SEPTEMBER 16, 2024
No. 24-1113 (and consolidated cases)

IN THE
United States Court of Appeals
for the District of Columbia Circuit

TIKTOK INC. and BYTEDANCE LTD.
Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of
the United States,
Respondent.

caption continued on inside cover

On Petitions for Review of Constitutionality of
the Protecting Americans from Foreign Adversary Controlled
Applications Act

**APPENDIX TO BRIEF OF PETITIONERS
TIKTOK INC. AND BYTEDANCE LTD.
Volume III of III (Pages 530–834)**

Andrew J. Pincus
Avi M. Kupfer
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3220
apincus@mayerbrown.com

*Counsel for Petitioners
TikTok Inc. and ByteDance Ltd.
(continued on inside cover)*

Alexander A. Berengaut
Counsel of Record
David M. Zions
Megan A. Crowley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
aberengaut@cov.com

BRIAN FIREBAUGH et al.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the
United States,

Respondent.

BASED Politics Inc.,

Petitioner,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the
United States,

Respondent.

John E. Hall
Anders Linderot
S. Conrad Scott
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018
(212) 841-1000

Counsel for Petitioners
TikTok Inc. and ByteDance Ltd.

TABLE OF CONTENTS

Volume I

H.R. Comm. on Energy & Com., <i>Protecting Americans from Foreign Adversary Controlled Applications Act</i> , H.R. Rep. No. 118-417 (2024)	1
<i>Legislation to Protect American Data and National Security from Foreign Adversaries: Hearing Before the Comm. on Energy & Com.</i> , 118th Cong. (2024) (excerpts)	19
170 Cong. Rec. H1164 (daily ed. Mar. 13, 2024)	39
170 Cong. Rec. S2629 (daily ed. Apr. 8, 2024) (excerpts)	48
170 Cong. Rec. H2561 (daily ed. Apr. 20, 2024) (excerpts)	71
170 Cong. Rec. S2943 (daily ed. Apr. 23, 2024) (excerpts)	98
Declaration of Alexander A. Berengaut	148
Ex. A: Document Entitled “Threat Posed by TikTok (Department of Justice - March 6, 2024)”	155
Ex. B: Draft National Security Agreement (Aug. 23, 2022) (redacted version; full version filed under seal)	157

Volume II

Declaration of Alexander A. Berengaut (continued)	
Ex. C: Governance Presentation to CFIUS (Sept. 17, 2021)	261
Ex. D: Protected Data Presentation to CFIUS (Oct. 13, 2021) (redacted version; full version filed under seal)	277
Ex. E: Content Moderation Presentation to CFIUS (Nov. 29, 2021)	306
Ex. F: Source Code Presentation to CFIUS (Nov. 30, 2021) (redacted version; full version filed under seal)	339

Ex. G: Content Assurance Process Summary (Apr. 26, 2022)	357
Ex. H: Letter from D. Fagan and M. Leiter to Hon. W. Adeyamo (Dec. 28, 2022)	359
Ex. I: Letter from E. Andersen to Hon. W. Adeyamo and Hon. L. Monaco (Feb. 25, 2023)	363
Ex. J: Email Exchange Between D. Fagan and M. Leiter and B. Reissaus (Mar. 2023)	366
Ex. K: Email from D. Fagan and M. Leiter to B. Reissaus (Apr. 27, 2023)	372
Ex. L: NSA Updates Presentation to CFIUS (May 23, 2023)	374
Ex. M: NSA Updates Presentation to CFIUS (Sept. 8, 2023)	385
Ex. N: Letter from D. Fagan and M. Leiter to D. Newman (Apr. 1, 2024) (redacted version; full version filed under seal)	412

Volume III

Declaration of Alexander A. Berengaut (continued)

Ex. O: Nicholas Kaufman et al., U.S.-China Econ. & Sec. Rev. Comm'n, Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes (Apr. 14, 2023)	530
Ex. P: Statements by Members of Congress	540
Transcript of Interview with Rep. Mike Gallagher, Fox News (Nov. 16, 2023)	541
House Comm. on the Chinese Communist Party, Press Release, Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok (Mar. 5, 2024)	544

Transcript of Interview with Reps. Mike Gallagher and Krishnamoorthi, CNN (Mar. 7, 2024).....	548
Sen. Tom Cotton (@SenTomCotton), X, https://x.com/SenTomCotton/status/1766875766111732082 , https://perma.cc/UY6H-4ZCY (Mar. 10, 2024)	553
Transcript of Interview with Rep. Raja Krishnamoorthi, Meet the Press (Mar. 12, 2024).....	554
Sapna Maheshawri et al., <i>House Passes Bill to Force TikTok Sale from Chinese Owner or Ban the App</i> , N.Y. Times (Mar. 13, 2024)	558
Transcript of Interview with Sen. Mark Warner, Fox News (Mar. 14, 2024) (excerpts)	565
Transcript of Interview with Rep. Mike Gallagher, Fox News (Mar. 16, 2024)	572
Jane Coaston, <i>What the TikTok Bill Is Really About, According to a Leading Republican</i> , N.Y. Times (Apr. 1, 2024).....	577
Sapna Maheshwari et al., <i>‘Thunder Run’: Behind Lawmakers’ Secretive Push to Pass the TikTok Bill</i> , N.Y. Times (Apr. 24, 2024).....	584
Transcript of Keynote Conversation Between Secretary of State Anthony Blinken and Sen. Mitt Romney, McCain Institute (May 3, 2024) (excerpts)	593
Prem Thakker et al., <i>In No Labels Call, Josh Gottheimer, Mike Lawler, and University Trustees Agree: FBI Should Investigate Campus Protests</i> , The Intercept (May 4, 2024) (excerpts).....	597
Transcript of Interview with Rep. Elise Stefanik, Maria Bartiromo (May 5, 2024) (excerpts)	599

Sen. John Fetterman (@SenFettermanPA), X, https://x.com/SenFettermanPA/status/ 1787891840022139280, https://perma.cc/2BW9-Z78H (May 7, 2024).....	609
Ex. Q: Paul Mozur et al., <i>TikTok Deal Is Complicated by New Rules From China Over Tech Exports</i> , N.Y. Times (Aug. 29, 2020).....	610
Ex. R: Xinhua News Agency, <i>Planned TikTok Deal Entails China’s Approval Under Revised Catalogue: Expert</i> , XinhuaNet (Aug. 30, 2020)	614
Ex. S: Letter from Sen. Charles E. Schumer (Apr. 5, 2024)	617
Ex. T: Rachel Dobkin, <i>Mike Johnson’s Letter Sparks New Flood of Republican Backlash</i> , Newsweek (Apr. 17, 2024)	620
Ex. U: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (excerpts).....	625
European Commission, <i>DSA: Very Large Online Platforms and Search Engines</i> , https://digital-strategy. ec. europa. eu/en/policies/dsa-vlops, https://perma.cc/49D9- F2UZ (last accessed June 17, 2024).....	626
Digital Services Act, 2022 O.J. (L 277) (excerpts)	632
Declaration of Randal S. Milch	643
Ex. 1: Summary of Divestitures Reviewed.....	688
Appx. A: Curriculum Vitae	705
Appx. B: Examples of Verizon’s Divestitures of Highly Integrated Assets	711
Declaration of Christopher P. Simkins.....	719
Appx. 1: Curriculum Vitae.....	758

Declaration of Steven Weber.....	760
Appx. 1: Curriculum Vitae.....	790
Declaration of Adam Presser	799

Exhibit O



Prepared by the research staff of the
U.S.-China Economic and Security Review Commission (USCC.gov)

April 14, 2023

Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes

Nicholas Kaufman, Policy Analyst, Economics and Trade

This Issue Brief details the challenges posed by Chinese “fast fashion” platforms, including exploitation of trade loopholes; concerns about production processes, sourcing relationships, product safety, and use of forced labor; and violations of intellectual property rights. These platforms primarily rely on U.S. consumers downloading and using Chinese apps to curate and deliver products. The primary focus of this Issue Brief is first mover Shein, about which the most data is available, with additional discussion of Temu, which has rapidly expanded its U.S. market presence in the past year. These firms’ commercial success has encouraged both established Chinese e-commerce platforms and startups to copy its model, posing risks and challenges to U.S. regulations, laws, and principles of market access.

Key Findings

Founded in 2008, Shein has emerged as a leading player for “fast fashion”^{*} consumers. Shein and similar companies work to market new, fashionable clothes from online and celebrity trends and deliver them quickly to consumers. Amid increased online purchases and fast-shifting trends influenced by social media, fast fashion has grown to a \$106.4 billion industry as of 2022.^{† 1} Using data analysis of its users’ search history and a consolidated and high-speed supply chain, Shein has outpaced competitors—including Zara and H&M—to take a dominant position in the U.S. market, a business model that other Chinese firms are seeking to replicate.

Numerous controversial practices have supported Shein and other Chinese e-commerce firms’ rapid growth. Investigations in 2022 alleged that Shein failed to declare that it had sourced cotton from Xinjiang for its products, a violation of the Uyghur Forced Labor Prevention Act. These claims are exacerbated by further reports of illegal labor conditions among the suppliers of Chinese fast fashion firms as well as findings that Shein products pose

^{*} Fast fashion is defined as cheap, trendy clothing that samples ideas from the catwalk or celebrity culture and turns them into garments at high speed to meet emerging consumer demand. Katherine Saxon, “Fast Fashion 2021 Guide – What It Means, Problems, and Examples,” *Fibre2Fashion*, August 2021. <https://www.fibre2fashion.com/industry-article/9163/fast-fashion-2021-guide-what-it-means-problems-and-examples>.

[†] China has accounted as the largest supplier to the U.S. apparel market through 2021; Beth Wright, “ANALYSIS: China Market Share of US Apparel Imports Rises after Four-Year Lull,” *Just Style*, March 4, 2022. <https://www.just-style.com/features/analysis-china-market-share-of-us-apparel-imports-rises-after-four-year-lull/>.

Disclaimer: The U.S.-China Economic and Security Review Commission was created by Congress to report on the national security implications of the bilateral trade and economic relationship between the United States and the People’s Republic of China. For more information, visit www.uscc.gov or follow the Commission on Twitter at @USCC_GOV.

This report is the product of research performed by professional staff of the U.S.-China Economic and Security Review Commission (USCC) and was prepared to support the ongoing research and deliberations of the Commission. Posting of this report to the Commission’s website is intended to promote greater awareness and understanding of developing issues for congressional staff and the public, in support of the Commission’s efforts to “monitor, investigate, and report” on U.S.-China economic relations and their implications for U.S. national security, as mandated by Public Law 106-398 (as subsequently modified in law, see uscc.gov/charter). The public release of this document does not imply an endorsement by the Commission, any individual Commissioner, or the Commission’s other professional staff, of the views or considerations raised in this staff-prepared report.

health hazards and environmental risks. Shein and several other Chinese fast fashion firms have also faced a high volume of copyright infringement accusations and lawsuits for intellectual property (IP) rights violations.

Shein and similar companies present a range of challenges to U.S. interests, including difficulties monitoring supply sources and obstacles in ensuring fair market practices with U.S. competitors. These companies also exploit trade de minimis import exemptions, through which firms make shipments to the United States that are below an \$800 value and are therefore not subject to import duties. Taken together, Shein and similar firms serve as a case study of Chinese e-commerce platforms outmaneuvering regulators to grow a dominant U.S. market presence.

Shein's Business Model: User Data and Supply Chain Integration

Shein's business model is distinguished by its reliance on tracking and analyzing user data. Founded by Chris Xu, a Chinese national with a background in search engine optimization, Shein draws on customer data and search history with the assistance of artificial intelligence (AI) algorithms to discern emerging fashion preferences and patterns.² With these rapid insights, Shein can begin manufacturing and delivering clothes to market ahead of competitors. To aid its data collection, the company's app also requests that users share their data and activity from other apps, including social media, in exchange for discounts and special deals on Shein products.³

While Shein has a supplier model built on tech-driven insights, it has struggled to protect user data. New York State fined Shein's owner, Zoetop—a Hong Kong-based LLC that owns Shein and sister company ROMWE—\$1.9 million in 2022 for mishandling credit card and other personal information following an investigation of a 2018 cyberattack that exposed the user data of 39 million accounts, including 800,000 users in New York.⁴ The office of the New York attorney general found that Zoetop had misled consumers about the extent of its data breach, had notified “only a fraction” of affected users that data credentials had been compromised, and had not reset the login credentials or otherwise taken steps to protect many of the exposed accounts.^{* 5}

Aside from anticipating trends, Shein's success also hinges on its ability to deliver products to consumers on a compressed timeline and at low cost. The company's integrated supply chain enables it to bring clothes to market in about five to seven days, when its competitors may take three weeks or longer.⁶ While Shein initially marketed products it purchased from third parties, it has built a sizeable exclusive supplier base in Guangdong Province, allowing it to improve manufacturing and delivery times.[†] According to a 2021 report by United Kingdom (UK)-based Channel 4, nearly half of the clothing suppliers in Guangzhou are partnered with Shein.⁷ This control over its own supply enables Shein to produce small batches of apparel quickly, rather than the typical practice of placing bulk orders, as U.S. firms do. Shein may produce as few as 50 pieces of clothing in its first production batch in order to accelerate delivery to buyers.⁸

Although founded in China, Shein does not sell domestically, instead marketing products exclusively abroad. Its presence has grown considerably in the United States over the last three years. With an aggressive digital and social media advertising campaign complemented by the expansion of online buying during the COVID-19 pandemic, Shein's market share of fast fashion sales in the United States rose from 18 percent in March 2020 to 40 percent in March 2022.⁹ By November 2022, Shein accounted for 50 percent of all fast fashion sales in the United States, ahead of brands H&M (16 percent) and Zara (13 percent).¹⁰ After surging past Tiktok, Instagram, and Twitter to briefly become the most downloaded app in the United States in May 2022, Shein maintained its growing popularity,

^{*} Of the leaked New York resident accounts, 375,000 were via Shein accounts, and 255,294 New York residents were not notified about the breach, according to the New York attorney general's office. Zoetop did not detect the intrusion until it was later notified by its payment processor that its systems appeared to have been compromised. In addition, Zoetop's public statements about the breach misrepresented the breach's size and scope. For example, Zoetop falsely stated that only 6.4 million consumers were affected by the breach and that the company was working notifying all of the impacted customers. Zoetop also represented, falsely, that it “ha[d] seen no evidence that [customer] credit card information was taken from [its] systems.” Two years later, Zoetop found customer login credentials for ROMWE accounts available on the dark web. New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers' Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.

[†] Shein utilizes a distributed network of suppliers across Guangdong Province and has steadily accumulated more than 200 contracted manufacturers near its major shipping hub in Guangzhou. These contractors are directly fed direction from Shein on production details and batch size in order to produce Shein products on an expedited timeline. Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.

finishing the year as the most downloaded platform for beauty and fashion across the U.S. application marketplace.¹¹ With 27 million downloads, Shein had more than double second-place Nike's 12.5 million downloads.¹²

The experience of Shein's expanding presence in the United States runs counter to that of U.S. e-commerce platforms in China.* Major digital and e-commerce firms face staunch regulatory barriers establishing operations, including onerous censorship restrictions and stiff legal regulations regarding cybersecurity.¹³ These market and non-market barriers forced Amazon to close down its Chinese marketplace in 2019.¹⁴

Chinese e-Commerce on U.S. Social Media

Social media increasingly plays a central role in the marketing of goods to U.S. consumers. In 2022, U.S. firms spent an estimated \$56 billion promoting their products on social networks.¹⁵ Half of Gen Z (18–25) and Millennial (26–41) consumers made purchases directly via social media platforms, according to the 2022 U.S. Digital Trust Survey.¹⁶

Among Chinese e-commerce firms, Shein and Temu—another China-based fast fashion app—are particularly well positioned to exploit social media platforms as a key conduit to U.S. consumers. Shein has more than 250 million followers across its social media channels.¹⁷ The “#shein” TikTok tag has over 3.3 billion views.¹⁸ Temu has invested heavily in social media marketing, purchasing 8,900 ads across Meta platforms in January 2023 alone.¹⁹

Both Shein and Temu partner closely with social media influencers. In a standardized application process on its website, Shein seeks influencer partnerships in exchange for shopping perks, bonuses, and exposure to its “community of 1M+ followers.”²⁰ Temu, which requires applicants to have at least 300 followers, similarly offers shopping perks and rewards.²¹ Influencers are encouraged to post “haul” videos of Shein and Temu products on U.S. social media platforms, where they are shown trying on clothes and other accessories and recommending products to followers.

Controversies in Shein's Business Practices

Several concerning patterns and practices have aided Shein's market approach.

- *Forced labor.* Shein cotton apparel sourcing practices appear to be in direct violation of the Uyghur Forced Labor Prevention Act. A Bloomberg investigation published in November 2022 cross-referenced climate and weather signatures on cotton fabrics used in clothing from Shein to determine that they originated in Xinjiang.[†] ²² The Uyghur Forced Labor Prevention Act bans the use of Xinjiang cotton in imported clothing unless the supplier can definitively prove that the cotton was not a product of forced labor, a step that Shein has not taken.[‡] ²³
- *Other exploitative labor practices and labor violations.* Outside of concerns about forced labor, a 2022 investigation by Channel 4 found a pattern of labor practice violations at Shein-affiliated factories in Guangzhou.²⁴ In one factory, workers were paid the equivalent of \$556 a month to make 500 garments a

* While no U.S. fast-fashion company has attempted market expansion into China comparable to Shein or Temu's inroads in the U.S. market, the experience of U.S. e-commerce companies in China is noteworthy due to the Chinese government's strict regulation of all internet companies and expanded control of the e-commerce market. Bien Perez, “China's E-Commerce Crackdown: Timeline of Beijing's Actions to Bring Tech Giants in Line with National Policy,” *South China Morning Post*, November 22, 2021. <https://www.scmp.com/tech/policy/article/3156719/chinas-e-commerce-crackdown-timeline-beijings-actions-bring-tech-giants>.

[†] Bloomberg contracted Agroislab GmbH, a lab in Germany, to test the items using stable isotope analysis. This process measures variations in the isotopes of carbon, oxygen, and hydrogen in the cotton's fibers to determine the climate characteristics and altitude of the region where it was grown. Shein's cotton was compared with two fabric samples from Xinjiang and. The first batch of Shein garments tested, which included pants and a blouse, matched the Xinjiang samples with only slight variations. Sheridan Prasso, “Shein's Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

[‡] Xinjiang Province is the source of 87 percent of Chinese cotton as of 2021. U.S. importers bought about \$8.4 million worth of cotton products from China in 2022, despite restrictions; Sheridan Prasso, “Shein's Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

day.²⁵ Workers had their first month's pay withheld in order to ensure worker retention. In another factory, workers had no base pay and were instead paid 4 cents a garment. These workers were fined heavily for mistakes in stitching or sewing.²⁶ The report further found workers in Shein factories working 18-hour workdays with one day off a month, clear violations of both Chinese labor laws and Shein's own supplier Code of Conduct.²⁷ Shein has faced other recent accusations of violating labor laws. Reuters reported in 2021 that Shein made false statements and lacked disclosures regarding its labor conditions, in violation of the UK's Modern Slavery Act.²⁸ A 2021 report from Public Eye, a Swiss Human Rights watchdog, described six Shein-affiliated factories without suitable fire exits and workers placed on extended working hours of about 75 hours a week with no overtime pay, another violation of Chinese labor law.²⁹

- *Health hazards.* The environmental and health impacts of Shein products are also facing scrutiny. A CBC Marketplace investigation found Shein clothing materials containing high levels of potentially hazardous chemicals, including lead, perfluoroalkyl (PFA), and phthalates.*³⁰ Health Canada tested a Shein jacket for toddlers and found it to have 20 times the amount of lead considered safe for children, while a purse from Shein contained over five times the accepted level for children.³¹ Environmental group Greenpeace also released a study alleging that various chemicals used in Shein products exceeded the level permitted by EU regulations.³²
- *Climate and environmental impact.* The UN Environmental Program estimates that due to its high-volume output, the fashion industry is responsible for 10 percent of annual global carbon emissions, more than all international flights and maritime shipping combined. At its current rate of growth, the fashion industry's greenhouse gas emissions will surge more than 50 percent by 2030.³³ Shein and other fast fashion platforms are exacerbating this trend by supplying higher volumes of cheaply produced clothing. A Bloomberg report found that Shein products contain 95.2 percent new plastics rather than recycled materials, while the large volume of shipments and low reuse rate among Shein products increases textile waste.³⁴ Good on You, which ranks the environmental impact of fashion companies, gave Shein its lowest rating.³⁵
- *Copyright infringement.* Shein and other Chinese e-commerce platforms and their suppliers have been met with numerous claims that they consistently violate U.S. IP law, with the *Wall Street Journal* reporting in 2022 that Shein in particular had over 50 outstanding federal cases over three years levied against it alleging trademark or copyright infringement.³⁶ In a June 2021 case, AirWear International, the parent company of shoe seller Dr. Martens, filed a lawsuit against Shein for its alleged "clear intent to sell counterfeits" and for copying the company's designs.³⁷ Complaints and cases against Shein range from major U.S. designers and retailers like Ralph Lauren to independent artists who claim Shein suppliers have used their designs on Shein clothing without permission. Independent designers who earn more of their income online are particularly vulnerable, as they have fewer resources with which to pursue legal action against Shein and its suppliers.³⁸
- *Avoiding tariffs and customs inspections.* Shein clothing and accessories average about \$11 per item.³⁹ This under-market pricing means Shein is exempt from the standard 16.5 percent import duty and 7.5 percent tariff specific to China.⁴⁰ De minimis packages are also exempt from customs inspection, allowing Shein to ship directly to consumers and helping the company avoid scrutiny over its cotton sourcing. Shein also benefits from a tax break in China: in response to the escalating U.S.-China trade dispute, in 2018 China waived export tariffs for direct-to-consumer businesses.⁴¹

* Research involving humans suggest that exposure to high levels of these PFAs and phthalates may pose risks of liver and kidney damage; Agency for Toxic Substance and Disease Registry, "What are the health effects of PFAS?" *Center for Disease Control*, November 1, 2022. <https://www.atsdr.cdc.gov/pfas/health-effects/index.html>. New Jersey Department of Health, *Hazardous Substance Fact Sheet*, May 2010. <https://nj.gov/health/eoh/rtkweb/documents/fs/1454.pdf>.

De Minimis Packages from China Evade Tariffs

Chinese e-commerce's growth in the United States has been aided by exploitation of favorable import regulations, especially the high de minimis threshold for U.S. customs inspection and tariffs. A de minimis threshold demarcates the value below which goods are considered too small to be subject to tariffs or most inspections. In the United States, this threshold was raised from \$200 to \$800 in 2016.⁴² By contrast, it is roughly \$7 (renminbi [RMB] 50) in China.⁴³

A sizeable majority of de minimis packages, which increased from 410.5 million packages in fiscal year (FY) 2018 to 685.1 million packages in FY 2022, came from China.⁴⁴ This correlates closely with the rise of e-commerce deliveries from China to the United States.⁴⁵ Shipments of de minimis packages from China in 2021 were about seven times the amount of Canada, the second-largest shipper of de minimis packages to the United States.⁴⁶ Customs data indicate that in 2022, more than 10 percent of Chinese imports by value now arrive as de minimis shipments, up from well under 1 percent a decade ago. In 2021, the Federal Reserve Bank of New York estimated that the U.S. Department of the Treasury loses as much as \$10 billion a year in tariffs through tariff strategies like de minimis.⁴⁷

Temu, Others Follow Shein's Model

Temu has replicated Shein's process of quickly manufacturing and shipping clothing to U.S. consumers. Temu recently sponsored two advertisements that aired during Super Bowl LVII at a cost of approximately \$14 million dollars, causing a 45 percent surge in downloads of its app and a daily active user jump of 20 percent on the day of the Super Bowl.⁴⁸ As of March 2023, Temu and Shein rank in the top five free apps on the Apple Store, ahead of retailers Amazon and Walmart.⁴⁹

Like Shein, Temu's success raises flags about its business practices. Temu's lack of affiliation with established brands has brought concerns of product quality as well as accusations of copyright infringement. As of April 2023, Temu has received 235 complaints in the last year with the Better Business Bureau, earning a 2.1 out of 5 stars customer rating.⁵⁰ PDD Holdings, Temu's parent company that operates the related e-commerce platform Pinduoduo in China,* was accused by China Labor Watch of "extreme overtime," requiring employees to work 380 hours per month.⁵¹ The company faced protests online after several worker deaths in 2021.⁵² Additionally, in April 2023, CNN reported that multiple cybersecurity teams found sophisticated malware on Pinduoduo's mobile app for Google Android devices. The malware enabled the Pinduoduo app to bypass user security permissions and access private messages, change settings, view data from other apps, and prevent uninstallation. The investigation followed Google's suspension of the app from the Google Play store in March 2023.[†] ⁵³

Numerous other established and emerging Chinese e-commerce firms seek to penetrate the U.S. market by modeling their strategies on Shein and Temu's businesses. LightInTheBox, an established Chinese e-commerce firm listed on the New York Stock Exchange since 2013, has invested heavily in a social media strategy that mimics Shein's. With the help of a New York-based advertising agency, LightInTheBox has now partnered with more than 2,000 influencers, and the company's products reach 200 million people via influencer-posted content.⁵⁴ Clothing e-commerce is a surging Chinese industry. Chinese state media outlet Sixth Tone reported that there are more than ten other startup-style Chinese firms founded since 2019 emulating Shein's business model and expanding their U.S. presence, including Cider, Urbanic, ChicV, Doublefs, Cupshe, and JollyChic. Though none have the market share of Shein or Temu, all similarly offer products at comparable prices with expedited delivery times.⁵⁵ Their

* PDD Holdings Inc. changed its name from Pinduoduo Inc. at an annual shareholders' meeting on February 8, 2023. PDD Holdings Inc., "Form 6-K: Report of Foreign Private Issuer Pursuant to Rule 13a-16 Or 15d-16 Under the Securities Exchange Act Of 1934," *U.S. Securities Exchange Commission*, February 9, 2023, https://www.sec.gov/Archives/edgar/data/1737806/000110465923014742/tm235930d1_6k.htm.

† Sergey Toshin, director of the app security company Oversecured, found that the Pinduoduo app had exploited about 50 vulnerabilities on the Android operating system. According to CNN, Pinduoduo company insiders said the malware was intentionally developed to spy on users and competitors to boost sales. Following reports that the app included malware, the company disbanded the engineering team charged with developing malware and reportedly transferred most of them to Temu. Nectar Gan, Yong Xiong, and Juliana Liu, "'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, say experts," *CNN*, April 2, 2023, <https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html>.

rapid proliferation raises concerns they will rely on controversial practices similar to those of Shein and Temu to undercut competitors and gain a foothold in the United States.

Considerations for Congress

Given the rapid increase in the market share of Shein and other Chinese e-commerce firms in the United States, the U.S. government should be vigilant in ensuring that these firms adhere to U.S. laws and regulations and are not granted unfair advantages over U.S. firms. Congress can help safeguard U.S. interests by addressing the following gaps in U.S. policy to respond to the business models and practices of Shein and other Chinese e-commerce firms.

- *Shein and perhaps other Chinese fast fashion firms appear to be sourcing goods in violation of the Uyghur Forced Labor Prevention Act.* The investigation by Bloomberg News tracing cotton fibers to Xinjiang highlights not only the platform's likely violation of U.S. law but also that the U.S. government does not have tools to effectively screen most e-commerce shipments from China. Packages that enter the United States, including the millions that enter below the de minimis threshold, are frequently not inspected. Those that are inspected are often subject to rudimentary visual checks without the technology or screening to trace fabric origin and other violations. Without the proper staffing and technological tools, U.S. customs officials are poorly positioned to identify and cease low-cost shipments that violate U.S. laws and regulations.
- *Chinese e-commerce platforms and suppliers routinely violate U.S. IP rights laws, and the consequences they face are insufficient to deter future violations.* Several U.S. firms, from large brands to in-home studios, have singled out Chinese firms for infringing on their copyrights. This is a particular issue for independent artists who have their designs used without permission by Shein suppliers or other Chinese e-commerce platforms and suppliers, as they may not have the resources to pursue legal remedies.
- *Current customs and tariff levels disproportionately benefit Chinese e-commerce firms.* The de minimis exemption level of \$800 allows for packages shipped to the United States under that level to avoid inspection and existing tariffs. Shein and other e-commerce firms are uniquely positioned to exploit this exemption, as their products are shipped individually and nearly all fall below the de minimis threshold.

Past Congressional and State Efforts on Chinese e-Commerce

Congress and at least one state government have already taken steps to evaluate and address the problematic practices of Chinese fast fashion firms and other Chinese e-commerce platforms.

- In February 2023, Senators Bill Cassidy (R-LA), Elizabeth Warren (D-MA), and Sheldon Whitehouse (D-RI) wrote to Shein's CEO seeking information on its alleged sourcing of Xinjiang cotton. The letter requested a response within 30 days.⁵⁶
- The COMPETE Act of 2022 passed by the House in the 117th Congress included a provision to remove de minimis privileges for goods sourced from nonmarket economies with known IP violations, including China.⁵⁷ The bill sought to effectively close the de minimis loophole that both Shein and Temu exploit when importing goods into the United States.⁵⁸ After reconciliation in conference committees, however, the final CHIPS and Science Act did not include language addressing de minimis thresholds.
- At the state level, New York State's Fashion Sustainability and Social Accountability Act would more closely monitor clothing sourcing and environmental impact. The act would severely limit the market access of Shein and Temu in New York State. The act was reintroduced to the State Assembly in February 2023, with stronger provisions for legally binding environmental and labor standards in the fast fashion industry.⁵⁹

Endnotes

- ¹ Cision PR Newswire, “Fast Fashion Global Market Report 2023,” February 17, 2023. <https://www.prnewswire.com/news-releases/fast-fashion-global-market-report-2023-301749153.html>.
- ² Isabella Fish, “Inside Shein: Exclusive Interview with Chinese Fast Fashion Giant,” *Drapers*, November 2, 2022. <https://www.drapersonline.com/insight/inside-shein-exclusive-interview-with-chinese-fast-fashion-giant>; Daniel Langer, “How China Will Use AI to Master the Luxury Market,” *Jing Daily*, December 20, 2021. <https://jingdaily.com/china-luxury-artificial-intelligence-shein/>.
- ³ Daxue Consulting, “Shein’s Market Strategy: How the Chinese Fashion Brand Is Conquering the West,” July 6, 2022. <https://daxueconsulting.com/shein-market-strategy/>.
- ⁴ Olivia Powell, “SHEIN Fined US\$1.9mn Over Data Breach Affecting 39 Million Customers,” *Cyber Security Hub*, October 14, 2021. <https://www.cshub.com/attacks/news/shein-fined-us19mn-over-data-breach-affecting-39-million-customers>; New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers’ Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.
- ⁵ BBC, “Shein Owner Zoetop Fined \$1.9m over Data Breach Response,” October 14, 2022. <https://www.bbc.com/news/technology-63255661>; New York State Office of the Attorney General, *Attorney General James Secures \$1.9 Million from E-Commerce SHEIN and ROMWE Owner Zoetop for Failing to Protect Consumers’ Data*, October 12, 2022. <https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop>.
- ⁶ Jerren Gan, “Here’s Why You Should Never Shop at Shein No Matter What,” *Age of Awareness*, July 14, 2021. <https://medium.com/age-of-awareness/heres-why-you-should-never-shop-at-shein-no-matter-what-8140d285cf4b>.
- ⁷ Emma Burleigh, “After a UK Documentary Revealed Abuses, Shein Says It Will Spend \$15 Million Improving Labor Conditions,” *Observer*, December 16, 2022. <https://observer.com/2022/12/after-a-uk-documentary-revealed-abuses-shein-says-it-will-spend-15-million-improving-labor-conditions>; Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- ⁸ Bloomberg News, “Fast-Fashion Upstarts Are Using Shein’s Own Strategies against It,” November 6, 2022. <https://www.bloomberg.com/news/articles/2022-11-06/fashion-retailer-shein-s-competitors-are-copying-its-super-fast-business-model?sref=mxblZFb4>.
- ⁹ Lynn Beyrouthy, “Market Share of the Leading Fast Fashion Companies in the U.S. 2020-2022,” March 28, 2023. <https://www.statista.com/statistics/1341506/fast-fashion-market-share-us/>.
- ¹⁰ Janine Perri, “Shein Holds Largest U.S. Fast Fashion Market Share,” *Bloomberg Second Measure*, January 4, 2023. <https://secondmeasure.com/datapoints/fast-fashion-market-share-us-consumer-spending-data-shein-hm-zara/>.
- ¹¹ MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>; Statista, “Most Downloaded Fashion & Beauty Apps in the U.S. 2022,” March 21, 2023. <https://www.statista.com/statistics/1212274/fastest-growing-fast-fashion-retailers-apps-in-the-us/>; MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>.
- ¹² Statista, “Most Downloaded Fashion & Beauty Apps in the U.S. 2022,” March 21, 2023. <https://www.statista.com/statistics/1212274/fastest-growing-fast-fashion-retailers-apps-in-the-us/>; MarketPlace Pulse, “Shein Is the Most-Downloaded App in the U.S.,” *Marketplace Pulse*, May 3, 2022. <https://www.marketplacepulse.com/articles/shein-is-the-most-downloaded-app-in-the-us>.
- ¹³ Paul Mozur and Carolyn Zhang, “Silicon Valley Giants Confront New Walls in China,” *New York Times*, July 22, 2017. <https://www.nytimes.com/2017/07/22/technology/in-china-silicon-valley-giants-confront-new-walls.html?mcubz=0>.
- ¹⁴ Bloomberg News, “Amazon Is Preparing to Close a Chinese E-Commerce Store,” April 18, 2019. <https://www.bloomberg.com/news/articles/2019-04-17/amazon-is-said-to-prepare-closing-of-chinese-e-commerce-store?sref=mxblZFb4>.
- ¹⁵ Statista, “Social Network Ad Spending in the U.S. from 2016-2022,” January 10, 2023. <https://www.statista.com/statistics/736971/social-media-ad-spend-usa/>.
- ¹⁶ Sara Lebow, “Half of Younger Consumers Buy Products on Social Media,” *Insider Intelligence*, October 26, 2022. <https://www.insiderintelligence.com/content/half-of-younger-consumers-buy-products-on-social-media>.
- ¹⁷ Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.
- ¹⁸ Veronika Bondarenko, “TikTok Fashion Favorite Shein Considers a Big Step,” *Street*, July 15, 2022. <https://www.thestreet.com/investing/tiktok-fashion-favorite-shein-considers-a-big-step>.
- ¹⁹ Sarah Perez, “Shopping app Temu is using TikTok’s strategy to keep its No. 1 spot on App Store,” *Tech Crunch*, January 23, 2023. <https://techcrunch.com/2023/01/23/shopping-app-temu-is-using-tiktoks-strategy-to-keep-its-no-1-spot-on-app-store/>.
- ²⁰ Shein, “Shein Influencer Program.” <https://us.shein.com/campaign/sheglaminfluencerprogram?lang=us>.
- ²¹ Temu, “Become a Temu Influencer.” <https://www.temu.com/influencer-collaboration.html>.
- ²² Sheridan Prasso, “Shein’s Cotton Tied to Chinese Region Accused of Forced Labor,” *Bloomberg News*, November 20, 2022. <https://www.bloomberg.com/news/features/2022-11-21/shein-s-cotton-clothes-tied-to-xinjiang-china-region-accused-of-forced-labor?sref=mxblZFb4>.

- ²³ United States Customs and Border Protection, *Uyghur Forced Labor Prevention Act*, December 23, 2021. <https://www.cbp.gov/trade/forced-labor/UFLPA>.
- ²⁴ Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- ²⁵ Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- ²⁶ Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- ²⁷ Channel 4, “Inside the Shein Machine: UNTOLD,” October 17, 2022. <https://www.channel4.com/programmes/inside-the-shein-machine-untold>.
- ²⁸ Victoria Waldersee, “EXCLUSIVE Chinese Retailer Shein Lacks Disclosures, Made False Statements about Factories,” *Reuters*, August 6, 2021. <https://www.reuters.com/business/retail-consumer/exclusive-chinese-retailer-shein-lacks-disclosures-made-false-statements-about-2021-08-06/>.
- ²⁹ *Public Eye*, “Toiling Away for Shein,” November 2021. <https://stories.publiceye.ch/en/shein/>.
- ³⁰ Jenny Cowley, Stephanie Matteis, and Charlise Agro, “Experts Warn of High Levels of Chemicals in Clothes by Some Fast-Fashion Retailers,” *CBC News*, October 1, 2021. <https://www.cbc.ca/news/business/marketplace-fast-fashion-chemicals-1.6193385>.
- ³¹ Stephanie Matteis and Jenny Cowley, “Health Canada Recalls Toxic Shein Kids’ Jacket Following CBC Investigation,” *CBC*, December 9, 2021. <https://www.cbc.ca/news/canada/health-canada-recall-shein-kids-jacket-1.6279903>; Jenny Cowley, Stephanie Matteis, and Charlise Agro, “Experts Warn of High Levels of Chemicals in Clothes by Some Fast-Fashion Retailers,” *CBC*, October 1, 2021. <https://www.cbc.ca/news/business/marketplace-fast-fashion-chemicals-1.6193385>.
- ³² *Greenpeace International*, “Taking the Shine off SHEIN: Hazardous Chemicals in SHEIN Products Break EU Regulations, New Report Finds,” November 23, 2022. <https://www.greenpeace.org/international/press-release/56979/taking-the-shine-off-shein-hazardous-chemicals-in-shein-products-break-eu-regulations-new-report-finds/>.
- ³³ *World Bank*, “How Much Do Our Wardrobes Cost to the Environment?” September 23, 2019. <https://www.worldbank.org/en/news/feature/2019/09/23/costo-moda-medio-ambiente>.
- ³⁴ Rachael Dottle and Jackie Gu, “The Global Glut of Clothing Is an Environmental Crisis,” *Bloomberg News*, February 23, 2022. <https://www.bloomberg.com/graphics/2022-fashion-industry-environmental-impact/?sref=mxblZFb4>.
- ³⁵ Good on You, “Shein,” March, 2023. <https://directory.goodonyou.eco/brand/shein>.
- ³⁶ Dan Strumpf, “China’s Fast-Fashion Giant Shein Faces Dozens of Lawsuits Alleging Design Theft,” *Wall Street Journal*, July 3, 2022. <https://www.wsj.com/articles/chinas-fast-fashion-giant-shein-faces-dozens-of-lawsuits-alleging-design-theft-11656840601>.
- ³⁷ *The Fashion Law*, “Shein Owner Zoetop Claims Dr. Martens Trademarks Are Generic,” October 26, 2021. <https://www.thefashionlaw.com/in-response-to-airwair-lawsuit-shein-owner-zoetop-claims-dr-martens-trademarks-are-generic/>.
- ³⁸ Dan Strumpf, “China’s Fast-Fashion Giant Shein Faces Dozens of Lawsuits Alleging Design Theft,” *Wall Street Journal*, July 3, 2022. <https://www.wsj.com/articles/chinas-fast-fashion-giant-shein-faces-dozens-of-lawsuits-alleging-design-theft-11656840601>.
- ³⁹ Lora Jones, “Shein: The Secretive Chinese Brand Dressing Gen Z,” *BBC*, November 9, 2021. <https://www.bbc.com/news/business-59163278>.
- ⁴⁰ Kenneth Rapoza, “How a U.S. Trade Loophole Called ‘De Minimis’ Is China’s ‘Free Trade Deal,’” *Forbes*, February 19, 2023. <https://www.forbes.com/sites/kenrapoza/2023/02/19/how-a-us-trade-loophole-called-de-minimis-is-chinas-free-trade-deal/?sh=508503b64c9b>; Bloomberg News, “How Trump’s Trade War Built Shein, China’s First Global Fashion Giant,” June 14, 2021. <https://www.bloomberg.com/news/articles/2021-06-14/online-fashion-giant-shein-emerged-from-china-thanks-to-donald-trump-s-trade-war?sref=mxblZFb4>.
- ⁴¹ David Morse, “The Pleasure Island of Shein,” *Coalition for a Prosperous America*, February 9, 2023. <https://prosperousamerica.org/the-pleasure-island-of-shein/>.
- ⁴² FTI Consulting, “Outcome of ‘De Minimis’ Will Have Major Effects on eCommerce Importations and the U.S. FTZ Program,” May 16, 2022. <https://www.fticonsulting.com/insights/articles/outcome-de-minimis-effects-ecommerce-importations-us-ftz>.
- ⁴³ Alavara, “De Minimis Value: A Minimum Value Defined by a Country Required to Apply Customs Duty and Tax Rates on Imported Goods.” <https://www.alavara.com/us/en/learn/cross-border-resources/de-minimis-threshold-table.html>.
- ⁴⁴ U.S. Customs and Border Protection, *Trade Statistics*. <https://www.cbp.gov/newsroom/stats/trade>.
- ⁴⁵ Kenneth Rapoza, “How a U.S. Trade Loophole Called ‘De Minimis’ Is China’s ‘Free Trade Deal,’” *Forbes*, February 19, 2023. <https://www.forbes.com/sites/kenrapoza/2023/02/19/how-a-us-trade-loophole-called-de-minimis-is-chinas-free-trade-deal/?sh=5fa293544c9b>.
- ⁴⁶ United States Customs and Border Protection, “SECTION 321 DE MINIMIS SHIPMENTS FISCAL YEAR 2018 to 2021 STATISTICS,” *United States Customs and Border Protection*, October, 2022. www.cbp.gov/sites/default/files/assets/documents/2022-Oct/FY2018-2021_De%20Minimis%20Statistics%20update.pdf.
- ⁴⁷ Josh Zumbrun, “The \$67 Billion Tariff Dodge That’s Undermining U.S. Trade Policy,” *Wall Street Journal*, April 25, 2022. <https://www.wsj.com/articles/the-67-billion-tariff-dodge-thats-undermining-u-s-trade-policy-di-minimis-rule-customs-tourists-11650897161>.
- ⁴⁸ Vidhi Choudhary, “After a Successful Super Bowl Ad, Temu’s Growth Is Outpacing Rivals Like Target,” *Modern Retail*, February 21, 2023. <https://www.modernretail.co/technology/after-a-successful-super-bowl-ad-temus-growth-is-outpacing-rivals-like-target/>.
- ⁴⁹ Apple, “Top Charts.” <https://apps.apple.com/us/charts/iphone/top-free-apps/36>.
- ⁵⁰ Better Business Bureau, “Temu.” <https://www.bbb.org/us/ma/boston/profile/online-shopping/temucom-0021-553943>.
- ⁵¹ Wilfred Chan, “Chinese Behemoth Pinduoduo to Take on Amazon in US – with Even Worse Labor Practices,” *Guardian*, August 25, 2022. <https://www.theguardian.com/technology/2022/aug/25/pinduoduo-us-labor-practices-worker-conditions>.

- ⁵² Vivian Wang, “Worker Deaths Put Big Tech in China under Scrutiny,” *New York Times*, February 1, 2021. <https://www.nytimes.com/2021/02/01/business/china-technology-worker-deaths.html>.
- ⁵³ CNN, “‘I’ve never seen anything like this:’ One of China’s most popular apps has the ability to spy on its users, say experts,” *CNN*, April 2, 2023. <https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html>.
- ⁵⁴ The Setters, “LightInTheBox.” <https://thesetters.agency/cases/case2/lightinthebox>.
- ⁵⁵ China Service Association, “2021-2022 年中国服装电子商务发展报告” (“2021-2022 China’s Clothing e-Commerce Development Report”), *China Garment Association*, May 23, 2022. Translation. [https://www.sixthtone.com/news/1009020/becoming-shein-chinese-retailers-eye-the-global-fast-fashion-market](http://webcache.googleusercontent.com/search?q=cache:oCFzsQ0k_gsJ:www.cnga.org.cn/html/shouye/remenzixun/2022/0523/54504.html%3F1653324274&cd=1&hl=en&ct=clnk&gl=us; Jiang Yaling, “Becoming Shein: Chinese Retailers Eye the Global Fast-Fashion Market,” <i>Sixth Tone</i>, November 19, 2021. <a href=).
- ⁵⁶ Office of Bill Cassidy, “Cassidy, Warren, Whitehouse Press SHEIN On Connection to Chinese Slave Labor Supply Chains,” *Office of Bill Cassidy*, February 9, 2023. <https://www.cassidy.senate.gov/newsroom/press-releases/cassidy-warren-whitehouse-press-shein-on-connection-to-chinese-slave-labor-supply-chains>.
- ⁵⁷ Braumiller Law Group, “Understanding the America Competes Act of 2022 - What Upcoming Major Changes to International Trade Law Should You Know About?” *Braumiller Law Group*. <https://www.lexology.com/library/detail.aspx?g=cdf14301-3330-496f-96af-f17d9e2e25a0>.
- ⁵⁸ Congressman Earl Blumenauer, “THE IMPORT SECURITY AND FAIRNESS ACT,” *Congressman Earl Blumenauer*, blumenauer.house.gov/sites/evo-subsites/blumenauer-evo.house.gov/files/One%20Pager%20-%20Import%20Security%20and%20Fairness%20Act.pdf.
- ⁵⁹ Kaley Roshitch, “Albany Bound: ‘Fashion Act’ Supporters Hope to Stir Renewed Support,” *WWD*, March 8, 2023, <https://wwd.com/sustainability/business/new-york-fashion-act-supporters-albany-sustainability-bills-1235576182/>; Nicole Grenfield, “New York Is Exposing the Fashion Industry for What It Is: a Climate Nightmare,” *NRDC*, February 13, 2023. <https://www.nrdc.org/stories/new-york-exposing-fashion-industry-what-it-climate-nightmare>.

Exhibit P

REP. MIKE GALLAGHER INTERVIEWED ON FOX NEWS (Nov. 16, 2023)

President Biden: The United States will continue to compete vigorously with the PRC. But we'll manage that competition responsibly so it doesn't veer into conflict or accidental conflict.

Anchor: So that from late last night, California, Northern California President Biden talking to reporters for about 20 minutes after his high stakes one-on-one meeting with the Chinese President Xi yesterday afternoon. The two leaders meeting face-to-face — first time in about a year that summit Northern California. Mike Gallagher is a Republican out of Wisconsin, chairman of the House China Committee. And Sir, thank you for your time and good morning to you.

So they spoke for what, 3 1/2 hours or so and while this was happening the Chinese Foreign Ministry put out a statement about Taiwan. And then at the end of the press conference last night, this is what President Biden was asked, about President Xi still being what he considered a dictator.

Question from Journalist: After today would you still refer to President Xi as a dictator? This is a term that you used earlier this year.

President Biden: Well, look, he is! I mean he's a dictator in the sense that he's a guy who runs a country, that is a communist country based on a form of government totally different than ours.

Anchor: Before that, there was a lot of nice words between the two. How did you read it based on the output from California?

Congressman Gallagher: Well, first I have to say that President Biden is correct. Xi Jinping is a dictator. When John Kerry, who was in these meetings, was asked whether Xi was a dictator, he refused to answer and instead said that Xi is a major decider. So I expect the President's handlers will be trying to clean that up.

As for the meeting itself, it's important to understand that getting this meeting has been the focus of U.S. foreign policy for the past year. The stakes were very high and thus far all we have are promises of future talks and potentially new pandas coming back to the D.C. Zoo. I'm afraid that's incredibly disappointing because we've taken our foot off the gas when it comes to things like sanctioning Chinese officials for egregious human rights abuses, pushing back against this unprecedented pressure against Taiwan, transparency around the spy balloon, or the origins of COVID. So it came at a great cost to even get to this meeting, and I hope that more will come out of it. Though I do support the establishment of a military-to-military communication channel, that alone won't be enough to deter PLA invasion of Taiwan.

Martha MacCallum: So, Congressman, you know it, it seems to me that the alliances that have been growing in the world, you see North Korea, Iran, Russia, China. And so it's extremely important that the United States strengthen its ties — Australia, Japan

and other countries in the region, which of course China does not want to see. So that's sort of the meat of where this reconstruction of the geopolitical world is right now. Do you think they talked about that at all?

Congressman
Gallagher:

I quite honestly don't know if that was the subject of the conversation. I will say a lot of the most important things that happened at APEC had nothing to do with Biden and Xi's conversation, but were precisely conversations among the allies, some of whom you just referenced. There was a trilateral meeting between Japan, us, and South Korea. There was a Quad meeting that was reportedly very constructive. To your broader point though, we need to push back against CCP aggression in concert with our regional allies. It is the goal of the CCP to sever our treaty alliances in the region and ultimately to push us out of the Pacific all the way back to Hawaii as step one in a multi step effort to achieve global domination and undermine American leadership. All the more reason why we not only need to reinforce existing alliances but look to create new ones and bring partners more firmly into the camp of the free world.

Anchor:

Just to put a button on this, what the statement said — I mean while the summit is happening OK — Taiwan — the question of Taiwan is the most important and most sensitive issue in China-US relations. End Quote on that. I wanna move to this TikTok story. Martha, we've been talking about this all morning. Go for it.

Martha
MacCallum:

So this disturbing trend on TikTok, Congressman Gallagher, of mostly young people, the ones that I saw, sharing Osama bin Laden's letter to America that he wrote the year after 9/11 to sort of describe all of the reasons for what he did. And try to justify the attacks on 9/11. And these people responding, to this letter, which has now been taken down, saying things like he was right, this is mind blowing, my mind is now open, are so deeply disturbing to me as I watched them this morning and I would imagine that if as people start to get a look at this, they will be very disturbed as well. Let's watch some of this.

TikTok posts:

Girl!

What?

They found the letter!

What letter?

The letter!

What letter!?

Osama's letter.

So I just read a letter to America and I will never look at life the same.

I feel like I'm going through like an existential crisis right now.

So this is a really good example of narrative control.

Martha
MacCallum:

You know, Congressman Gallagher, they go on to say terrorism was sold to the American people as if these terrorists just woke up and said one morning, we hate America, let's go kill as many people as we can. And they conclude — one of them — that it was just our government failing. 9/11 was just our government failing other countries. What would you say about this, sir?

Congressman
Gallagher:

Well, these people are of course massive idiots. I just came from watching the footage that the Israeli Embassy compiled about the October 7th attack. It is horrific. You're seeing Salafi jihadists — Hamas in this case, but Al Qaeda was a Salafi jihadist organization — kill babies, behead innocent civilians with garden hoes. These images are incredibly disturbing and show the true face of evil. So for someone on TikTok to somehow suggest that this is America's fault or that bin Laden who killed thousands of innocent Americans was right, is absolutely disgusting and further evidence that we need to ban TikTok or force a sale before a Chinese controlled app before the Chinese Communist Party checkmates the free world by controlling the dominant media platform in America that can spread this dangerous disgusting nonsense. It is time for a ban or a forced sale before it's too late.

Anchor:

Just to put an emphasis on this — the letter is 21 years old and people felt like it just came out today. Mike Gallagher, thank you for your time. I know your feelings on TikTok and we'll see whether or not eventually you get your way. Thank you, sir.



Enter keywords

Search

[Home](#) / [Media](#) / [Press Releases](#)

Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans From Foreign Adversary Controlled Applications, Including TikTok

March 5, 2024 · [Press Release](#)

WASHINGTON, D.C.-- Rep. Mike Gallagher (R-WI) and Rep. Raja Krishnamoorthi (D-IL), Chairman and Ranking Member of the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, today introduced the Protecting Americans from Foreign Adversary Controlled Applications Act. The bill prevents app store availability or web hosting services in the U.S. for ByteDance-controlled applications, including TikTok, unless the application severs ties to entities like ByteDance that are subject to the control of a foreign adversary, as defined by Congress in Title 10.

In addition, the bill creates a process for the President to designate certain, specifically defined social media applications that are subject to the control of a foreign adversary—per Title 10—and pose a national security risk. Designated applications will face a prohibition on app store availability and web hosting services in the U.S. unless they sever ties to entities subject to the control of a foreign adversary through divestment.

The bill is co-led by House Republican Conference Chair Elise Stefanik (R-NY), Rep. Kathy Castor (D-FL), Rep. Bob Latta (R-OH), Rep. Andre Carson (D-IN), Rep. Kevin Hern (R-OK), Rep. Seth Moulton (D-MA), Rep. Chip Roy (R-TX), Rep. Mikie Sherrill (D-NJ), Rep. Neal Dunn (R-FL). Rep. Haley Stevens (D-MI), Rep. Ralph Norman (R-SC), Rep. Jake Auchincloss (D-MA), Rep. Kat Cammack (R-FL), Rep. Ritchie Torres (D-NY), Rep. John Moolenaar (R-MI), Rep. Shontell Brown (D-OH), Rep. Ashley Hinson (R-IA), and Rep. Josh Gottheimer (D-NJ). The bill is co-sponsored by Rep. Dusty Johnson (R-SD), Rep. Nancy Pelosi (D-CA), Rep. Carlos Gimenez (R-FL), Rep. Anna Eshoo (D-CA), Rep. Darin LaHood (R-IL), Rep. Chris Deluzio (D-PA), Rep. Timothy Walberg (R-MI), Rep. Marc Veasey (D-TX), Rep. Rick Allen (R-GA), Rep. Elissa Slotkin (D-MI), Rep. John Joyce (R-PA), Rep. Andrea Salinas (D-OR), Rep. Earl "Buddy" Carter (R-GA), Rep. Kweisi Mfume (D-MD), Rep. August Pfluger (R-TX), Rep. Hillary Scholten (D-MI), Rep. Dan Crenshaw (R-TX), Rep. Chris Pappas (D-NH), Rep. John Curtis (R-UT), Rep. Jonathan Jackson (D-IL), Rep. Brian Fitzpatrick (R-PA), Rep. Jim Costa (D-CA), Rep. Mark Alford (R-MO), Rep. Jake LaTurner (R-KS), Rep. Stephanie Bice (R-OK), Rep. Scott Fitzgerald (R. WI), Rep. Mike Lawler (R-NY), Rep. Claudia Tenney (R-NY), Rep. Jeff Van Drew (R-NJ), Rep. Mike Kelly (R-PA), Rep. Cory Mills (R-FL), Rep. Gus Bilirakis (R-FL), Rep. Brad Sherman (D-CA), Rep. Vern Buchanan (R-FL), and Rep. Victoria Spartz (R-IN).

“This is my message to TikTok: break up with the Chinese Communist Party or lose access to your American users,” **said Chairman Gallagher**. “America’s foremost adversary has no business controlling a dominant media platform in the United States. TikTok’s time in the United States is over unless it ends its relationship with CCP-controlled ByteDance.”

“So long as it is owned by ByteDance and thus required to collaborate with the CCP, TikTok poses critical threats to our national security. Our bipartisan legislation would protect American social media users by driving the

divestment of foreign adversary-controlled apps to ensure that Americans are protected from the digital surveillance and influence operations of regimes that could weaponize their personal data against them. Whether it's Russia or the CCP, this bill ensures the President has the tools he needs to press dangerous apps to divest and defend Americans' security and privacy against our adversaries," **said Ranking Member Krishnamoorthi.**

"TikTok is Communist Chinese malware that is poisoning the minds of our next generation and giving the CCP unfettered access to troves of Americans' data. I am proud to join Chairman Mike Gallagher in introducing the Protecting Americans from Foreign Adversary Controlled Applications Act to finally ban TikTok in the United States. From proliferating videos on how to cross our border illegally to supporting Osama Bin Laden's Letter to America, Communist China is using TikTok as a tool to spread dangerous propaganda that undermines American national security. We cannot allow the CCP to continue to harness this digital weapon," **said Rep. Stefanik.**

"In this day and age, we all know about the vast benefits – and vast risks – of our most popular social media platforms. Ensuring that foreign adversaries do not have the ability to control what we see and hear online is an important piece of what should be a bipartisan effort to make social media safer for all Americans. This bill would ensure that Tik Tok is no longer controlled, even indirectly, by the Chinese Communist Party, and does so in a responsible way, that doesn't take away Americans' favorite social media apps," **said Rep. Moulton.**

"The dangerous link between TikTok and the Chinese Communist Party has never been more apparent. When TikTok's CEO came before the Energy and Commerce Committee last year, he readily admitted to me that ByteDance employees in China have access to U.S. user data. This alone should serve as a wake-up call and alarm every single American – whether they're actively engaged on TikTok or not. TikTok and its ties to Communist China poses a clear and present danger to U.S. national security and is threatening the privacy of millions of Americans. I'm proud to help lead the bipartisan Protecting Americans from Foreign Adversary Controlled Applications Act, which will ban the app from the United States if TikTok is not divested by the Chinese Communist Party," **said Rep. Latta.**

"All Americans deserve access to information and media platforms that are free from the influence of hostile foreign actors like the Chinese Communist Party. But here are the facts: TikTok has been used by the CCP to silence free speech and dissent in the United States and abroad, to undermine democracy and our values, and to promote propaganda that is favorable to autocratic rulers like President Xi. In New Jersey, TikTok has banned users for posting content that brought awareness to the CCP's horrific genocide and forced labor of the Uyghur people. It's nothing short of dangerous that the CCP controls a key source of information for millions of Americans – including so many teenagers and children who've seen their mental health harmed by the app. This bipartisan legislation should be passed immediately to protect our democracy, our national security, and our kids," **said Rep. Sherrill.**

"The House Select Committee on the CCP and the House Energy & Commerce Committee have found alarming proof of our data being shared with our adversaries via applications developed by ByteDance," **said Rep. Dunn.** "I even asked the TikTok CEO point blank if ByteDance has spied on Americans on behalf of the CCP, and his response was 'I don't think spying is the right way to describe it.' This is outrageous. I took an oath to protect the American people and I'm proud to join this effort to ban applications that can be utilized and abused by our adversaries."

"Social media corporations are attention-fracking American youth and corroding our democracy. Congress needs to get tough on them -- but we can only do that if these corporations are subject to U.S. law. TikTok needs to answer to Congress, not Xi Jinping," **said Rep. Auchincloss.**

"TikTok is owned by the Chinese Communist Party and we cannot allow the CCP to indoctrinate our children. This strong bipartisan legislation is an important step forward in making sure social media apps owned by foreign adversaries are prohibited from doing business in America. I encourage all Americans using TikTok to strongly consider the personal risks of having their data owned by the Chinese Communist Party and hope they will stop using the app as this bipartisan legislation moves forward," **said Rep. Moolenaar.**

"Congress can no longer afford to ignore the growing threat posed by foreign adversary-controlled applications like TikTok," **said Rep. Torres.** "TikTok not only jeopardizes our national security but also threaten our fundamental freedoms by allowing adversaries to surveil and influence the American public under the guise of a social media platform. The Protecting Americans from Foreign Adversary Controlled Applications Act is a crucial step in safeguarding our nation. We must act swiftly and decisively to protect our citizens and preserve our sovereignty."

"Not only is the CCP-controlled TikTok an immense national security risk to our country, it is also poisoning the minds of our youth every day on a massive scale. China is our enemy, and we need to start acting like it. I am proud to partner with Representatives Gallagher and Krishnamoorthi on this bipartisan bill to ban the distribution of TikTok in the US. This legislation will make our country better off and more secure," **said Rep. Roy.**

"The Chinese Communist Party has made it abundantly clear that it is willing to leverage technology to collect data on our children and all US citizens. Using TikTok, China has the ability to control what an entire generation of kids

sees and consumes every single day,” said Rep. Gottheimer. “It’s time we fight back against TikTok’s information invasion against America’s families. In the wrong hands, this data is an enormous asset to the Chinese Communist Party — a known adversary — and their malign activities.”

“Any technology—apps, software, language models—owned by foreign adversaries are unequivocal threats to our national security. We have every right to protect Americans’ constitutional rights, data privacy, and national security, and it’s only become clear over the last several years how dangerous these foreign-owned tech platforms truly are,” said Rep. Cammack. “As a member of the Energy & Commerce Committee which deals heavily in the telecom and tech space, I don’t take this decision lightly. I’m grateful to Chairman Gallagher and the Select Committee on the CCP for spearheading this effort and I look forward to the bipartisan support this effort will garner to keep the U.S. safe from malign influence, adversarial infiltration, espionage, and beyond.”

“TikTok is CCP spyware used by the regime to steal Americans’ data and push harmful propaganda, including content showing migrants how to illegally cross our Southern Border, supporting Hamas terrorists, and whitewashing 9/11. Bottom line: TikTok needs to completely cut ties with the CCP or it will no longer be available in the United States. It is past time to dismantle the CCP’s top propaganda and spyware tool,” said Rep. Hinson.

Summary: Applications like TikTok that are controlled by foreign adversaries pose an unacceptable risk to U.S. national security. Such apps allow our adversaries to surveil and influence the American public, both through the data we produce and the information we share and consume.

This legislation addresses the threat in two ways. First, it prevents app store availability or web hosting services in the U.S. for ByteDance-controlled applications, including TikTok, unless the application severs ties to entities like ByteDance that are subject to the control of a foreign adversary, as defined by Congress in Title 10. The bill provides ByteDance with a window of time to divest, and the bill’s prohibitions do not apply if it completes a qualified divestment. It also creates a process for the President to designate certain, specifically defined social media applications that are subject to the control of a foreign adversary—per Title 10—and pose a national security risk. Designated applications will face a prohibition on app store availability and web hosting services in the U.S. unless they sever ties to entities subject to the control of a foreign adversary through divestment. This bill addresses the immediate national security risks posed by TikTok and creates a process for the President to protect Americans’ national security and privacy from foreign adversary-controlled applications in the future.

Click [HERE](#) to read text of the bill.

What the Bill Does:

- **Incentivize Divestment of TikTok:** Unless TikTok is fully divested such that it is no longer controlled by a PRC-based entity, the application will face a prohibition in the U.S. from app store availability and web hosting services until such time as a divestment occurs.
- **Address the National Security Risks Posed by Other Applications Controlled by Foreign Adversary Companies:** Establishes a process for the President to designate other foreign adversary controlled social media applications—as defined by statute—that shall face a prohibition on app store availability and access to web hosting services in the United States unless they sever ties to the foreign adversary-controlled company. The President may exercise this authority if an application presents a national security threat, has over one million annual active users, and is under the control of a foreign adversary entity, as defined by statute.
- **Empower Users to Switch Platforms:** Designated applications must provide users with a copy of their data in a format that can be imported into an alternative social media application. All users would be able to download their data and content and transition to another platform.

What the Bill Does Not Do:

- **Punish Individual Social Media Users:** No enforcement action can be taken against individual users of an impacted app.
- **Censor Speech:** This legislation does not regulate speech. It is focused entirely on foreign adversary control—not the content of speech being shared. This bill only applies to specifically defined social media apps subject to the control of foreign adversaries, as defined by Congress.
- **Impact Apps That Sever Ties to Foreign Adversary-Controlled Entities:** An app, including TikTok, that severs ties with entities subject to the control of a foreign adversary is not impacted by any other provision of the bill.

TikTok

CQ Newsmaker Transcripts

Mar. 7, 2024

Mar. 07, 2024 Revised Final

Reps. Gallagher and Krishnamoorthi Interviewed on CNN

LIST OF SPEAKERS

JAKE TAPPER, CNN HOST:

In our tech lead now, **TikTok** influencers, beware. Today, a House committee voted on a bipartisan bill that could effectively ban the app in the United States if it gets passed by the entire House, then goes to the Senate, then the president signs it into law.

The legislation would force ByteDance. That's the name of **TikTok**'s parent company to sever ties with its host country China or be banned from US app stores.

The lawmakers behind the bill say apps that are controlled by foreign adversaries such as China, collect way too much information on the Americans who use them, use the apps, and posed security risks to the United States.

Joining us now, Republican Congressman Mike Gallagher and Democratic Congressman Raja Krishnamoorthi, the co-authors of the bill.

Mr. Chairman, let me start with you. There are more than 170 million **TikTok** users in the US. It's one of the most popular apps in the world.

What do you say to them if the US ends up banning **TikTok**? As I'm sure you've heard from a lot of them today, they are worried. They

REP. MIKE GALLAGHER (R-WI), CHAIRMAN, SELECT
COMMITTEE ON

CHINA:

Well, we hope that they will continue to be able to use the platform once TikTok makes the responsible decision to separate itself from ByteDance. TikTok can continue you need to exist in the United States as long as its not effectively controlled by the Chinese communist party.

That is the issue, and that will make for a better user experience. People won't have to worry about manipulation of algorithms. They won't have to worry about a hostile foreign adversary potentially manipulating the news that Americans consume.

And I would say the pressure campaign that TikTok put in place today where they forced the pop up on the app that called members of Congress and also told a lie that we were -- we were forcing an outright ban, which this bill is not proves the danger. They sort of proved the entire point. Imagine if those lies were allowed to spread on topics like our election or a foreign war.

So, that's what we're trying to guard against. And in our construct, users can continue to enjoy the app so long as we fix the owner appreciate problem.

TAPPER:

So, Congressman Krishnamoorthi, if it's not an outright ban, what is it exactly? And what would happen? Would the app disappear from people's phones or would it just stopping -- sold by Apple, et cetera?

REP. RAJA KRISHNAMOORTHY (D-IL):

Well, it's a forced sale. That's what -- you know, that's what's happened in the past. By the way, another app, the popular app called Grindr, was one its purchased by the Chinese and basically, the American federal government forced the sale of that particular app because again, the CCP has the access to very sensitive data about government officials and military officials.

And this is a much bigger problem with regard to **TikTok**. **TikTok** is owned by ByteDance. The editor in chief of ByteDance is himself the secretary of the very Chinese communist party cell embedded in the leadership of ByteDance. And his duty, according to him, is to make sure that **TikTok** and other products abide by correct political direction. And so that's why we took this app section today. The House Energy and Commerce Committee voted 50 to zero unanimously.

That has not happened with regard to any bill affecting this particular platform. And now we look forward to its passage in the House.

TAPPER:

So, Mr. Chairman, there's a First Amendment fight over this as well. The ACLU says that your legislation soon as a violation of free speech rights. The senior policy counsel at the organization says, quote, just because the bill sponsors claimed that banning **TikTok** isn't about suppressing speech, there's no denying that it would do just that. We strongly urge legislators to vote no on this unconstitutional bill, unquote.

Do you think that the national security threat outweighs whatever free speech issues there are out there?

GALLAGHER:

To be clear, I don't think our bill endangers any First Amendment issues at all. We're talking about foreign ownership and control of an app. And once that foreign ownership is addressed, not only will people be able to continue to say whatever they want on the app, you'll also have freedom of thought, freedom from fear that your thought might be manipulated because of the opaque algorithms.

And for that illogical claim that **TikTok** is making to be true than previous incidents where we've addressed ownership, for example, in the antitrust paradigm, would have had a massive First Amendment impact. The breakup of Bell in 1982 would have been one of the biggest further First Amendment issues in American history. But, of course, it wasn't.

So that's -- we've carefully worked on this bill for six months. We've worked with the White House to get technical assistance. We are very confident that this is a construct that avoids any issue like a bill of attainder does not infringe on freedom of speech. It's about foreign adversary control of the news and the ability to spy on Americans.

KRISHNAMOORTHY:

It's the same principle. Look, the First Amendment does not protect espionage. It does not protect the right to harm American national security. It's the same reason why under our laws, we prevent a certain portion of ownership of broadcast networks and certain media outlets.

It's the same reason why, for instance, a bookstore needs to comply with other rules, even though it sells books and protected First Amendment expression. And so, that is what is at issue here. We don't

want to sensor any type of content. This is not about a content-specific law. This is about the manner in which the CCP controls ByteDance, the parent of the platform at issue.

TAPPER:

All right. Chairman Mike Gallagher and Congressman Raja Krishnamoorthi, the ranking Democrat on the Special Committee on the Chinese Communist Party, thank you so much.

Appreciate your taking the time to talk to us today.

KRISHNAMOORTHY:

Jake, thank you so much.

List of Speakers

REP. MIKE GALLAGHER (R-WI)

REP. RAJA KRISHNAMOORTHY (D-IL)

JAKE TAPPER, CNN HOST



← Post



Tom Cotton 
@SenTomCotton

TikTok exposes Americans' data to the Chinese government, exposes children to harmful content, and is a source of propaganda.

We should ban it in the U.S. or force it to be sold.



1:16 PM · Mar 10, 2024 · 54.2K Views

222 Reposts **43** Quotes **827** Likes **15** Bookmarks



New to X?



Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Relevant people



Tom Cotton ✓
@SenTomCotton

U.S. Senator proudly serving the state
of Arkansas.

Follow



Don't miss what's happening
People on X are the first to know.

Log in

Sign up

<https://x.com/SenTomCotton/status/1766875766111732082>

APP-553

REP. RAJA KRISHNAMOORTHY INTERVIEWED ON MEET THE PRESS**(March 12, 2024)****Yamiche Alcindor:**

Joining me now is democratic Congressman from Illinois, Representative Krishnamoorthi. He is the ranking member of the China Select Committee and he and Chairman Mike Gallagher introduced that bill that could ban TikTok. So thank you so much for being here, Congressman.

Rep. Krishnamoorthi:

Hey, thanks, Yamiche.

Yamiche Alcindor:

Now, it's still unclear when the Senate will take up your legislation, but I want to play for you what some senators are saying about your bill. Take a listen.

Sen. Lindsey Graham:

I understand people like TikTok. I would like to keep TikTok running but not have our data used by the communist Chinese.

Anchor:

How would you vote on this?

Sen. Lindsey Graham:

I don't know yet. I mean I'm just being honest with you. I am definitely conflicted.

Sen. Dick Durbin:

There's a lot of questions my colleagues are asking myself included. I haven't come to a final decision as to whether or not it should be banned.

Yamiche Alcindor:

So Congressman you just got a classified briefing this afternoon, what is your message to senators in particular who may be on the fence about this legislation?

Rep. Krishnamoorthi:

Well, first of all, this is not a ban. What we're calling for is a divestment of TikTok by ByteDance, its owner, which is controlled by the Chinese Communist Party. And really, this isn't about TikTok, it's about ByteDance. And I think that what we're hearing is the President wants this authority to be able to balance the legitimate concerns of people who are on the platform, who should continue to enjoy the platform, with the legitimate national security concerns that

have to do with our adversary, the CCP, and what it does in terms of its access to data as well as in manipulation of the algorithm on the platform.

Yamiche Alcindor:

Congressman, if they don't divest, you will ban them. And to be clear, you also put a six-month deadline on this. So explain how that how you square that with the idea that you put this ban, you put the consequence of the ban on the table. That was your decision.

Rep. Krishnamoorthi:

Yeah. So basically they would be suspended from being able to operate until they comply with the law. This is very common. We have various laws that basically prevent excess ownership with regard to broadcast outlets, telecom companies, even railroads. And so what we're saying here is that we need to comply with that particular law. They need to reduce their ownership to no more than a 20% stake in the company and at that point they would be in compliance.

Yamiche Alcindor:

I understand your view on that. I want to also add something about former President Trump. He said he believes that TikTok poses a national security risk. He initially supported banning it. I know you're saying it would be suspended. He also is reversing course here, he's flipping the script. How worried are you that President Trump and him not supporting this bill that it could tank it in the eleventh hour?

Rep. Krishnamoorthi:

Well, I think he's been flip flopping and then flipping. Just the other day he gave a rambling conversation with or interview with CNBC in which he said, you know, TikTok is absolutely a national security threat. I'm not really sure what exactly is motivating Donald Trump. Something tells me it has something to do with politics. Surprise, surprise. But the main point here is we have to do what is right. And what is right here is making sure that we ensure the divestment of the Chinese Communist Party and ByteDance with regard to TikTok.

Yamiche Alcindor:

Congressman, I also want to ask you about the constitutional issues that might be here. The ACLU has been critical of your bill, saying it would violate the First Amendment. They argue, quote, banning TikTok would have a profound implications for our constitutional right to free speech and free expression because millions of Americans rely on the app every day for

information, communication, advocacy and entertainment. So how would you respond to that argument? And are you concerned that this bill could end up being blocked by the courts because of those constitutional issues that the ACLU is bringing up?

Rep. Krishnamoorthi:

No, there is no right. There is no First Amendment right to espionage. No, there's no First Amendment right to harm our national security. There are a number of cases, including Supreme Court cases, that basically say that even in a situation where, for instance, a bookstore is not in compliance with laws of general application and even though obviously the authors and others who have the right to express themselves and the books contained in that bookstore should be able to sell them. If the bookstore is out of compliance, it's not allowed to operate until it's in compliance. And that's the situation here. Similarly, you know, broadcast outlets and other companies, we have foreign ownership limits or thresholds that can't be crossed. And I think that this is one of those situations where we don't want a foreign adversaries controlled social media app to basically harm our national security, while we want people to continue to express themselves on the platform. I think that this law achieves the balance and so people will be able to continue to do so. We have a precedent here. There was Grinder, which is a LGBTQ app that was owned at one time by a Chinese company. Because we realized that the Chinese Communist Party had access to the sensitive personal data of LGBTQ members of the military and the government, we required divestment. That happened without a hitch. It happened quickly because Grinder was a valuable social media app, just as TikTok is, and there was no disruption of service, which is what we would expect here as well.

Yamiche Alcindor:

Well Congressman you talked about TikTok being a sort of bookstore. What if the President was in that bookstore? You have President Biden's campaign. As you know, they've joined TikTok, in fact, their campaign posted a new video today. Doesn't that undermine in some ways your argument that this poses a national security threat if the President of the United States and his campaign is on it?

Rep. Krishnamoorthi:

Well, I'm not going to tell the President how to campaign. I don't have TikTok on my own personal phone and it's certainly banned from all government devices, but I think that everyone should use it very cautiously going forward. What I do know is what happened last

week illustrates exactly why we need this particular bill. You may be aware that our particular bill passed out of the Energy and Commerce Committee, which is the committee of jurisdiction here, 50 to nothing. That almost never happens, certainly not on the Energy and Commerce Committee. But the reason it happened is because TikTok, on the day of the vote decided to use a push notification and a pop up app — a pop up window on its app that required minor children in order to be able to use the app to call their member of Congress on the Energy and Commerce Committee to lobby against the bill in question. Well when they called these offices, they flooded those offices with phone calls. By the way, these minor children basically asked the question, what is Congress and what is a Congressman? And on top of that, in one case they impersonated the child of one of the legislators. In another case, they actually called the congressman's office and said I'm going to commit self harm unless you turn on my TikTok. And so this illustrated in one example exactly why this particular legislation is necessary. Today, Christopher Wray at the Worldwide Threats hearing said in the open hearing when I asked him about this particular example. He said he could not rule out that the CCP itself conducted this particular operation. So that is why we need this particular legislation.

Yamiche Alcindor:

We will certainly be watching this legislation. Thank you so much, Congressman, for your time.

Rep. Krishnamoorthi:

Thank you.

House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App

The legislation received wide bipartisan support, with both Republicans and Democrats showing an eagerness to appear tough on China.



By Sapna Maheshwari, David McCabe and Annie Karni

March 13, 2024

The House on Wednesday passed a bill with broad bipartisan support that would force TikTok's Chinese owner to either sell the hugely popular video app or have it banned in the United States.

The move escalates a showdown between Beijing and Washington over the control of a wide range of technologies that could affect national security, free speech and the social media industry.

Republican leaders fast-tracked the bill through the House with limited debate, and it passed on a lopsided vote of 352 to 65, reflecting widespread backing for legislation that would take direct aim at China in an election year.

The action came despite TikTok's efforts to mobilize its 170 million U.S. users against the measure, and amid the Biden administration's push to persuade lawmakers that Chinese ownership of the platform poses grave national security risks to the United States, including the ability to meddle in elections.

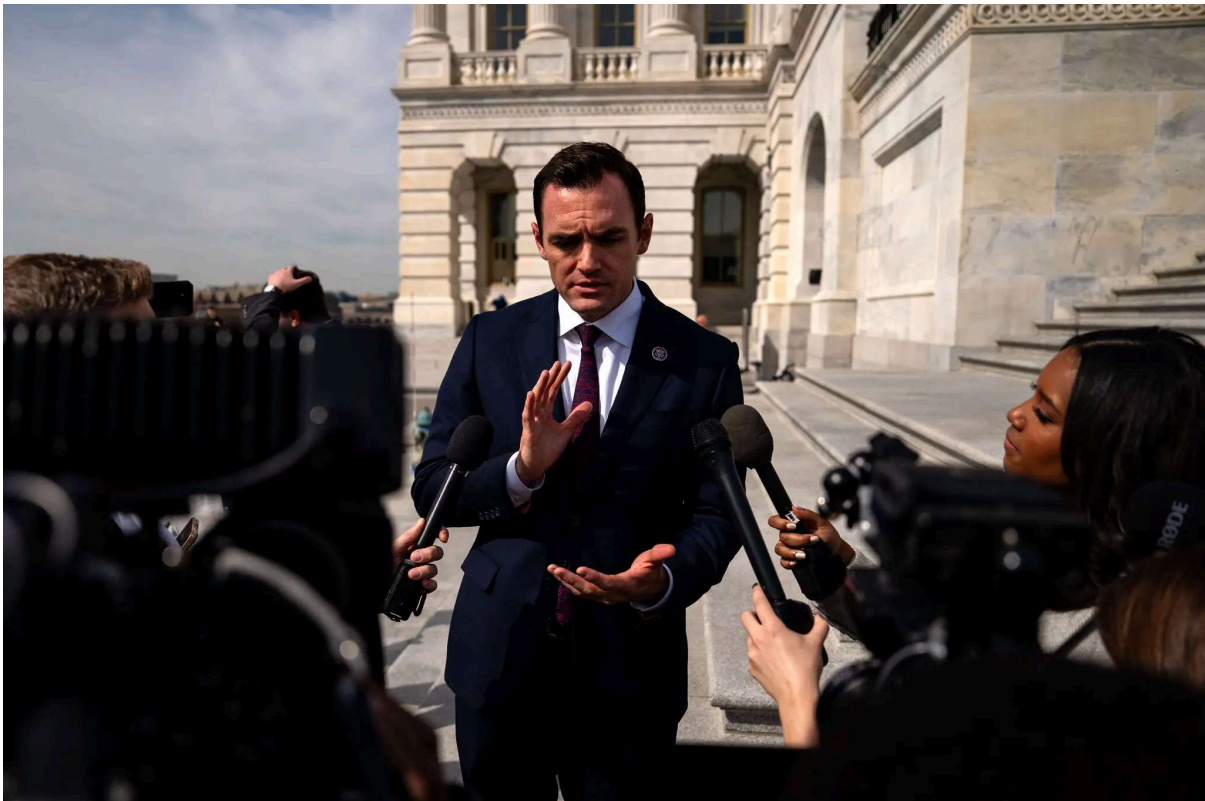
The result was a bipartisan coalition behind the measure that included Republicans, who defied former President Donald J. Trump in supporting it, and Democrats, who also fell in line behind a bill that President Biden has said he would sign.

The bill faces a difficult road to passage in the Senate, where Senator Chuck Schumer, Democrat of New York and the majority leader, has been noncommittal about bringing it to the floor for a vote and where some lawmakers have vowed to fight it. And even if it passes the Senate and becomes law, it is likely to face legal challenges.

But Wednesday's vote was the first time a measure that could widely ban TikTok for consumers was approved by a full chamber of Congress. The app has been under threat since 2020, with lawmakers increasingly arguing that Beijing's relationship with TikTok's parent company, ByteDance, raises national security risks. The bill is aimed at getting ByteDance to sell TikTok to non-Chinese owners within six months. The president would sign off on the sale if it resolved national security concerns. If that sale did not happen, the app would be banned.

Representative Mike Gallagher, the Wisconsin Republican who is among the lawmakers leading the bill, said on the floor before the vote that it "forces TikTok to break up with the Chinese Communist Party."

"This is a common-sense measure to protect our national security," he said.



APP-559

Representative Mike Gallagher, the Wisconsin Republican who is among the lawmakers behind the bill. Kent Nishimura for The New York Times

Alex Haurek, a spokesman for TikTok, said in a statement that the House “process was secret and the bill was jammed through for one reason: It’s a ban.”

“We are hopeful that the Senate will consider the facts, listen to their constituents, and realize the impact on the economy — seven million small businesses — and the 170 million Americans who use our service,” he added.

On Wednesday, before the House vote, Beijing condemned the push by U.S. lawmakers and rejected the notion that TikTok was a danger to the United States. At a daily press briefing, Wang Wenbin, a spokesman for China’s foreign ministry, accused Washington of “resorting to hegemonic moves when one could not succeed in fair competition.”

If the bill were to become law, it would likely deepen a cold war between the United States and China over the control of many important technologies, including solar panels, electric vehicles and semiconductors.

Mr. Biden has announced limitations on how U.S. financial firms can invest in Chinese companies and restricted the sale of Americans’ sensitive data like location and health information to data brokers that could sell it to China. Platforms like Facebook and YouTube are blocked in China, and Beijing said last year that it would oppose a sale of TikTok.

TikTok has said that it has gone to great lengths to protect U.S. user data and provide third-party oversight of the platform, and that no government can influence the company’s recommendation model. It has also said there is no proof that Beijing has used TikTok to obtain U.S. user data or to influence Americans’ views, two of the concerns lawmakers have cited.

In an unusually aggressive move for a technology company, TikTok urged users to call their representatives last week to protest the bill, saying, “This legislation has a predetermined outcome: a total ban of TikTok in the United States.”

TikTok has spent more than \$1 billion on an extensive plan known as Project Texas that aims to handle sensitive U.S. user data separately from the rest of the company's operations. That plan has for several years been under review by a panel known as the Committee on Foreign Investment in the United States, or CFIUS.

Two of the lawmakers behind the bill, Mr. Gallagher and Raja Krishnamoorthi, an Illinois Democrat, said last week that lawmakers were acting because CFIUS "hasn't solved the problem."

It's very unusual for a bill to garner broad bipartisan support but at the same time divide both parties. President Biden has said he would sign the bill into law, but top House leaders like Representative Katherine Clark of Massachusetts, the No. 2 Democrat in the House, voted against the bill. Mr. Trump said he opposed the bill, but many of his most stalwart allies in the House, like Representative Elise Stefanik of New York, the No. 4 Republican in the House, voted for it.

The vote came down to something of a free-for-all, with unusual alliances in support of and opposed to the bill. Representative Nancy Pelosi, Democrat of California and the former house speaker, sat in the chamber nodding along with hard-right Republicans like Representative Dan Crenshaw, Republican of Texas, as they outlined their support for the bill. At one point, she got up and crossed over to the Republican side of the aisle to confer with Representative Chip Roy, a hard-right Republican of Texas, who had vocally supported the bill on the floor.

Several Republicans and Democrats expressed their opposition to the bill based on free speech concerns and TikTok's popularity in the United States. Some legal experts have said that if the bill were to become law, it would probably face First Amendment scrutiny in the courts.

Representative Maxwell Frost, a Democrat of Florida, said on Tuesday that "not only am I no, but I'm a hell no." He said the legislation was an infringement of First Amendment rights. "I hear from students all the time that get their information,

the truth of what has happened in this country, from content creators on TikTok.” He said he was concerned about Americans’ data, but “this bill does not fix that problem.”



Representative Maxwell Frost at a news conference with TikTok creators on Capitol Hill on Tuesday. Haiyun Jiang for The New York Times

There wasn't any legislation last year in the aftermath of a fiery hearing with Shou Chew, TikTok's chief executive, despite bipartisan support to regulate the app. But concern among lawmakers has grown even more in recent months, with many of them saying that TikTok's content recommendations could be used for misinformation, a concern that has escalated in the United States since the Israel-Hamas war began.

“It was a lot of things in the interim, including Oct. 7, including the fact that the Osama bin Laden ‘Letter to America’ went viral on TikTok and the platform continued to show dramatic differences in content relative to other social media platforms,” Mr. Krishnamoorthi said in an interview.

There's also a chance that even if the bill is signed and survives court challenges, it could crumble under a new administration. Mr. Trump, who tried to ban TikTok or force its sale in 2020, publicly reversed his position on the app over the past week. In a television appearance on Monday, Mr. Trump said that the app was a national security threat, but that banning it would help Facebook, a platform the former president criticized.

"There are a lot of young kids on TikTok who will go crazy without it," he said.

Mr. Trump's administration had threatened to remove TikTok from American app stores if ByteDance did not sell its share in the app. ByteDance even seemed ready to sell a stake in the app to Walmart and Oracle, where executives were close to Mr. Trump.

That plan went awry in federal court. Multiple judges stopped Mr. Trump's proposed ban from taking effect.

Mr. Biden's administration has tried turning to a legislative solution. The White House provided "technical assistance" to Mr. Gallagher and Mr. Krishnamoorthi as they wrote their bill, Karine Jean-Pierre, the White House press secretary, said at a briefing last week. When the bill was introduced, a National Security Council spokesman quickly called the legislation "an important and welcome step to address" the threat of technology that imperils Americans' sensitive data.

The administration has repeatedly sent national security officials to Capitol Hill to privately make the case for the legislation and offer dire warnings on the risks of TikTok's current ownership. The White House briefed lawmakers before the 50 to 0 committee vote last week that advanced the bill to the full House.

On Tuesday, officials from the Federal Bureau of Investigation, the Office of the Director of National Intelligence and the Justice Department spoke with lawmakers in a classified briefing about national security concerns tied to TikTok.

Mr. Gallagher and Mr. Krishnamoorthi had previously sponsored a bill aimed at banning TikTok. The latest bill has been viewed as something of a last stand against the company for Mr. Gallagher, who recently said he would not run for a

fifth term because “the framers intended citizens to serve in Congress for a season and then return to their private lives.”

Sapna Maheshwari reports on TikTok, technology and emerging media companies. She has been a business reporter for more than a decade. Contact her at sapna@nytimes.com. More about Sapna Maheshwari

David McCabe covers tech policy. He joined The Times from Axios in 2019. More about David McCabe

Annie Karni is a congressional correspondent for The Times. She writes features and profiles, with a recent focus on House Republican leadership. More about Annie Karni

CQ Newsmaker Transcripts

Mar. 14, 2024

Mar. 14, 2024 Revised Final

Sen. Warner Interviewed on Fox News

LIST OF SPEAKERS

NEIL CAVUTO, FOX NEWS ANCHOR:

All right, you know what happened in the House.

In an overwhelming vote that was bipartisan, the move was, TikTok cannot be what it is right now, controlled by China, and that means ByteDance, the parent company of China, must unload it, divest it, as they say on Wall Street.

But it isn't getting the same reaction in the United States Senate. Again, Chuck Schumer has not even detailed if or even when the Senate will take it up.

Senator Mark Warner joins us right now. He is the Senate Intelligence Committee chairman.

Senator, good to have you.

Do you think the Senate should take up this issue?

SEN. MARK WARNER (D-VA):

Absolutely.

Neil, I have been on your show many, many times talking about the national security threat that is posed by having a platform that 170

million Americans use on average 90 minutes a day. China is collecting this data about lots of Americans.

And what is even more problematic for me is, the genius of TikTok is, it knows what you like before you know what you like. And a lot of young people get all their news. They could switch the algorithm a little bit and suddenly all the TikTok videos will be promoting that Taiwan ought to be part of China, or that Putin's right...

CAVUTO:

Right.

WARNER:

... on getting Ukraine. And I think...

CAVUTO:

No, all these examples you raised, you obviously eloquently put the key arguments here.

But it doesn't look like Chuck Schumer either agrees or sees the need to do something right now.

WARNER:

Well...

CAVUTO:

Now, that could change. Is it your understanding that it will and the Senate will take up the matter?

WARNER:

Well, listen, Neil, I know Senate never moves quickly on anything.

But my friends in the House, that was a huge vote, 352 votes. It was just yesterday. I think, Schumer, I have had preliminary conversations. Chair Cantwell on the Commerce Committee is going to have views. There may be things that need to be slightly altered or amended.

But I think anyone who cares about -- we have plenty of divisions in our country.

CAVUTO:

Yes.

WARNER:

We ought to be able to argue amongst ourselves, left and right, Republican, Democrat. We don't need the Chinese Communist Party dominating or influencing.

(CROSSTALK)

CAVUTO:

So, the sheer size of that vote, the sheer size of that vote in the House would maybe -- has maybe changed the thinking in the Senate, as far as you...

WARNER:

I think so.

CAVUTO:

OK.

WARNER:

I would say so.

(CROSSTALK)

CAVUTO:

So let me ask you about that then, Senator.

One other idea that's been bandied about, if ByteDance were to go ahead and divest itself of **TikTok**, no sure thing, that **TikTok** would essentially be for sale one way or the other. A lot of American names have come into play here. Oracle's name comes up, Microsoft, Meta, of course, the Facebook parent.

Do you have any concerns with any of those names?

WARNER:

Well, I have concerns about too much concentration, if this was acquired by another social media company.

And, frankly, that's all of our preference. If you like **TikTok**, if you're a social influencer on that, you want to be, and you make your living that way, that's great with me. It just ought to be a company that's not controlled by China.

So I was really glad to see Donald Trump's Treasury Secretary Steve Mnuchin put out word today that he was trying to put together a group of investors that could potentially buy this application. I think that he'd be great. He was one of the guys that first educated me on this issue.

And I know I have said this. I don't say this often, even on FOX, but, on TikTok, Donald Trump was right years ago in saying it was a national security threat. Now, he's changed his tune a little bit now.

CAVUTO:

Yes.

WARNER:

But his initial indication on this as a national security threat was right. And I think it would be great if a group of investors were to buy this.

So the service could still be extended. People could still get to see all the crazy and fun videos, but, ultimately, it would be with American or European or somebody other than Chinese ownership.

CAVUTO:

You know, it doesn't quite cut black and white, right, Senator? I mean, you mentioned Donald Trump changing his mind on this, that maybe we don't get rid of it for the time being or push to get rid of it.

But it is a hot political issue, or could be, right? Because 170 million Americans use this.

WARNER:

Yes.

CAVUTO:

Lopsidedly, they're young, and they don't want it to go away.

WARNER:

Well...

CAVUTO:

And that they might get ticked off and take it out on politicians who do push to have it go away.

WARNER:

I hear it. And that's why I say, let's not have it go away. Let's just not have the Communist Party of China pulling its strings.

I think...

CAVUTO:

But what do you -- how do you react when young people say, they don't care, Senator?

WARNER:

But...

CAVUTO:

They figure that everyone spies on them when they're online. It's not forgivable, don't get me wrong, but that they don't draw the distinction China doing it versus an American company doing it, as you're still being spied on.

How do you react to that? How do you talk to them?

WARNER:

Well, I would react a couple of ways.

One, that funny or inappropriate video two, five years from now, if somebody's trying to blackmail you from the Chinese spy services, I don't think you're going to want that to happen. And even if they don't care about the propaganda purposes, we would never let the Chinese Communist Party buy FOX News or MSNBC.

The idea that they have this propaganda channel that can affect Americans' views, again, we got plenty to fight about amongst ourselves.

CAVUTO:

Yes.

WARNER:

Let's not turn the reins over.

And one of the reasons that I think that something will happen is that we have done nothing on social media for years. I mean, the fact that we don't even have any kids online safety, again, broad bipartisan support for that, if we can't at least start with something that is this pervasive, controlled by an adversary of the United States, then all the things that folks think about Washington are true.

But I got a lot of hope; 352 people in the House, I didn't think you would get 352 House members to agree on anything.

CAVUTO:

No, you're quite right about that. You're quite right about it.

Let me ask you. You were mentioning the possibility how would we react to the Chinese where -- you first mentioned FOX News and

CQ Newsmaker Transcripts

Mar. 16, 2024

Mar. 16, 2024 Revised Final

Rep. Gallagher Interviewed on Fox News

LIST OF SPEAKERS

BRIAN KILMEADE, FOX NEWS CHANNEL HOST:

Joining us right now, the man who doesn't. He is leading the charge as Chairman of the House Select Committee on China. He's part of the reason there's over 300 votes in the House and it is now at the feet of the Senate. Congressman Mike Gallagher.

Congressman, your thoughts about the push back of the bill you helped push?

REP. MIKE GALLAGHER (R-WI):

Well, clearly, my colleagues who voted against it, whose criticism you just played didn't actually read the bill.

This is not a ban on speech. This is a ban on foreign adversary control on social media, which is particularly crucial given that TikTok is now a dominant news platform for kids, for Americans under the age of 30. Would we want the Chinese Communist Party to determine what news, what information we get to see?

It does not surprise me that members of the squad would want to use the app in order to get information on the conflict between Israel and Hamas right now because the information is purely one-sided, in favor of the genocidal death cult that is Hamas or if they want it to be

aspirational call.

This is the type of content we're seeing on a platform and imagine how it could be weaponized if we were debating something as critical as an authorization for the use of military force to defend Taiwan.

Look at what they did to try and stop this vote last week? Forced a pop-up notification on millions of users and then you had 11-year-olds calling Congress threatening to commit suicide if we took action.

That's just a taste of how this platform can be weaponized by the CCP in the future.

KILMEADE:

Chairman, do you believe that this is part of a bigger story? They've tried to kill us with fentanyl, not addict us, kill us with fentanyl, try to infiltrate our country and try to tell us what's important. And that is why in my view, you could tie that right to the protests on these college campuses. And through the streets, these young people who believe the Palestinian-Hamas cause is the place America should be right now.

GALLAGHER:

It's a part of something bigger, which Xi Jinping calls the smokeless battlefield. That is his ideological war against the West, a campaign designed to weaken America from within and pit Americans against Americans and get a generation to really loathe and hate their own country and thereby undermine any action.

We need to actually beat the Chinese Communist Party in this protracted competition, this new Cold War. Yes, it's absolutely part of

KILMEADE:

Chairman, I want you to hear this. Aishah Hasnie was able to catch up with the CEO who has worked in the Senate side to try to stop this vote before and by the way, this would be sell 80 percent of it, or you get banned within six months. Here's the exchange.

(BEGIN VIDEO CLIP)

AISHAH HASNIE, FOX NEWS CHANNEL CONGRESSIONAL
CORRESPONDENT:

Sir, why won't ByteDance just sell the company? That would avoid a ban. Why wouldn't you just sell?

SHOU ZI CHEW, CEO, **TIKTOK**:

The bill is 12 pages long. We have looked at it. It is not feasible to do whatever the bill thinks it does within the -- within the perimeter set out in the bill.

(END VIDEO CLIP)

KILMEADE:

What's he talking about, Chairman? What's not feasible about selling?

GALLAGHER:

Not only is it feasible, it's been done before. I mean, there was a similar issue related to the app Grindr and Chinese ownership of that and we forced divestitures all the time. We tackle ownership issues like this.

We have an entire Committee on Foreign Investment in the United States that deals with things like this. So he's not being honest. And the fundamental problem remains which is that he is beholden to ByteDance and ByteDance is beholden to the Chinese Communist Party and that's a risk that we can't take going forward.

KILMEADE:

People say, well what about the Fifth Amendment? What about the First Amendment? But people don't understand, this is China. This goes right back to China. If people say this is a Chinese company, but the Chinese government doesn't own it. What do you say to that?

GALLAGHER:

Well, the biggest threat to free expression or the first amendment would be Chinese ownership of a news platform in America and people can continue to post dance videos or political speech or campaign on the app so long as ByteDance separates from Tik Tok and TikTok separates from the Chinese Communist Party. They can continue to use the app, that's all we're talking about here.

There is no scenario in which this bill targets speech, content. It's about foreign adversary ownership narrowly defined. So in addition to getting free speech, in the new world in which TikTok is not controlled by the CCP, you can have something even better.

You can have freedom of thought, freedom from fear that the algorithm is being manipulated to mess with you. That's what we're after here and that's the world we want to live in.

KILMEADE:

We never should have allowed it to get a foothold in 2016, but we could change everything right now and 2024. Hopefully the president and the Senate has the courage to do it.

Chairman, thanks so much. Appreciate it.

GALLAGHER:

Thank you, sir.

KILMEADE:

You got it.

List of Speakers

REP. MIKE GALLAGHER (R-WI)

BRIAN KILMEADE, FOX NEWS CHANNEL HOST

JANE COASTON

What the TikTok Bill Is Really About, According to a Leading Republican

April 1, 2024



By Jane Coaston

Ms. Coaston is a contributing Opinion writer.

Last month, the House passed a bill that would require TikTok's parent company, ByteDance, to sell its U.S. business to a company without ties to the Chinese government or face a ban of the TikTok app in the United States.

In Washington, which has become increasingly hawkish toward the Chinese government, worries and fears about the Chinese Communist Party's role in ByteDance are widespread. But outside Capitol Hill, millions of people — especially younger Americans — use TikTok every day for entertainment and increasingly for search. Even beyond the potential speech or other legal issues, if this bill becomes law and a divestiture doesn't work, those people might be pretty surprised if they were no longer able to download or update the TikTok app.

Representative Mike Gallagher, Republican of Wisconsin, is a co-sponsor of the legislation. He's about to leave Congress, but if this becomes law, it will have an effect on social media and U.S.-China relations long after his departure. Many lawmakers in both parties are concerned about the effects of social media on teens. Mr. Gallagher's much more concerned about the Chinese government, and we

spoke about speech concerns, the message to authoritarian governments from a bill like this and how Donald Trump's fluctuating support affects the chances the bill will become reality.

This interview has been edited for length and clarity and is part of an Opinion Q. and A. series exploring modern conservatism today, its influence in society and politics and how and why it differs (and doesn't) from the conservative movement that most Americans thought they knew.

Jane Coaston: So what's the scenario with TikTok that you fear the most? Data theft, misinformation, tracking generations of Americans and then using their information and attention against them? Or something duller than what I'm imagining?

Representative Mike Gallagher: There are two threats. One is what you could call the espionage threat. It's data security — using the app to find Americans, exfiltrate data, track the location of journalists, etc. We have incidences of this happening already that are in the public domain. That's a serious threat, but I actually think the greater concern is the propaganda threat. If TikTok continues to establish itself as the dominant news platform in America and if the algorithm remains a black box and subject to the control of ByteDance and, by extension, the Chinese Communist Party, you're placing the control of information — like what information America's youth gets — in the hands of America's foremost adversary. And that's a risk I don't think we can afford to take. Obviously, there's well-established precedent when it comes to traditional media for foreign ownership, which is why we think a divestiture is the most prudent way to guard against both of those threats.

[In 2022, Forbes reported that TikTok employees pulled the IP addresses and user information of three reporters to monitor their whereabouts after the reporters published a critical article about ByteDance; TikTok said the employees were no longer employed by the company.]

Sign up for the Opinion Today newsletter Get expert analysis of the news and a guide to the big ideas shaping the world every weekday morning. Get it sent to your inbox.

Coaston: Let's say I'm 19 years old, I'm in college. I use TikTok for normal stuff. Make the case to me that there's a security risk.

Gallagher: We have already examples of TikTok, as I mentioned before, spying on journalists. TikTok has not been truthful about where its data was housed in the past, and using TikTok's own metrics when it comes to comparing content on that platform versus Instagram — recognizing it's not an apple-to-apples comparison, based on the different way the apps work — there are disparities that don't make any sense. It can't be explained away by sounding variables such as the fact that TikTok doesn't operate in India. And the closer you get to the topics that are sensitive to the Chinese Communist Party — whether it's Covid origins, whether it's the Uyghur genocide, whether it's Hong Kong, etc. — the disparities get more and more severe. Again, this gets back to the black box nature of the algorithm. But the other thing I would say to that 19-year-old who wants to continue to use TikTok, that's fine. In the scenario that our bill envisions, once the ownership structure changes, the national security concerns are substantially alleviated. I see no reason the user experience can not only continue but also improve.

[This year TikTok limited access to a tool that researchers used to track trending topics on the platform. In the past, groups like the Network Contagion Research Institute at Rutgers University have found that based on tags, certain topics, like protests about increasing antidemocratic measures in Hong Kong and reports of the confinement and forced labor of Uyghur Muslims in China, are underrepresented on TikTok compared with Instagram. TikTok has said that the Chinese government has no influence over the app.]

Coaston: How much have you used TikTok? Do you have a burner phone with TikTok on it, by any chance?

Gallagher: I do not. I don't really use social media at all. I have a Twitter staff account, but I made that decision about six years ago, I think, to remove myself personally from it. I don't have it on my phone. And that was more to me a matter of wanting to be effective, and I found myself not having the time I wanted to do deep thinking and writing and researching, and the minute I got off it, the more my productivity improved. Now, that's just me personally; I just don't find it useful. There are occasions when I would use Twitter to sort of monitor various Chinese Communist Party propaganda accounts during the pandemic. I became fascinated with what they were doing to spread kind of dangerous anti-American rhetoric on our platforms.

People will send me TikTok videos sometimes as examples, but I don't have the app even on a burner phone. I do think when we're talking about all this stuff — social media companies in America and China — a principle underlying all of it has to be reciprocity. As we have this debate about how and whether to regulate a foreign-adversary-controlled social media application in the United States, it's worth remembering that our social media applications are not allowed in China. There's just a basic lack of reciprocity, and your Chinese citizens don't have access to them. And yet we allow Chinese government officials to go all over YouTube, Facebook and X spreading lies about America. I think this is a microcosm with a broader lack of reciprocity in the entire U.S.-China relationship. And I do think, as a matter of principle, it puts us on firm ground to address this issue.

Coaston: Jameel Jaffer at the Knight First Amendment Institute recently said on X, "A U.S. TikTok ban would be a gift to authoritarian regimes around the world." There's also an argument that banning an app in the same way that the Chinese Communists do, as you just mentioned, is basically a propaganda win for China. How should conservative China hawks be thinking about the messages that this ban might send worldwide?

Gallagher: Which is why it's not structured as a ban and why TikTok lies about it being an outright ban. That argument backfired — and I think the push notification they forced on millions of users actually sort of proved our point about the concerns with how the tool could be weaponized to inject disinformation into the

American legislative process and the democratic process. The outcome we're trying to navigate toward is a divestiture or a sale or a separation. I actually think that's an outcome that American investors in ByteDance should want. We're not talking about an outright ban; we're trying to force a sale. Now, you need a mechanism to force the sale, to be sure. I also would disagree that the bill addresses content or speech; it's about conduct, specifically foreign adversary control of social media.

[TikTok has sent messages to users to call their representatives, which resulted in widespread calls to congressional offices.]

Coaston: So there are some Republican lawmakers who seem most concerned with the mental health of young people rather than something specific to Chinese ownership. In states like Utah, where I live, there are efforts to restrict teen social media usage more broadly. Are you in favor of that more expansive, less libertarian approach to social media and big tech for younger people? For adults?

Gallagher: Well, I think I need to caveat this: I share the concerns, but it's a separate issue than what this bill is trying to address. What I'm narrowly trying to address with this bill is foreign adversary control of a dominant social media platform and news platform in the United States. Now, once we address that issue, then we can have a bigger debate about the effect of social media more broadly to include American social media companies. I've been persuaded by Jonathan Haidt's work, both in the previous book he wrote with Greg Lukianoff, "The Coddling of the American Mind," and then Haidt's book that just came out, "The Anxious Generation," that it is strongly correlated with the skyrocketing rate of anxiety and depression that we're seeing among Gen Z. I think it's worthy of government attention. There's not an obvious government solution that I've been able to address. In fact, right now, my instinct is that it is my responsibility as a parent to set guardrails and not rely on the government to do it for me.

You could, however — and I think this is where Haidt's analysis has been very persuasive — entertain raising the internet age of adulthood. And that is something that I haven't seen a piece of legislation yet that I'm ready to co-sponsor, but the

idea makes sense to me, and I think there would be government authority to do that if we decided to do that. But again, that is not what this bill is about.

The other idea, which I think is sensible but doesn't lend itself to federal legislation — though there might be state and local efforts at the school-district level — is finding a way to incentivize, if not mandate, phone-free schools. Haidt's analysis is very good at highlighting the benefits of doing that. But again, that's not something I would legislate as a member of Congress, if that makes sense. As a parent, I'm terrified about the corrosive impact of social media. I even see it among my colleagues, and I referenced my own experience and how social media, I think, really sapped my own productivity. I think there's a way in which it precludes us from having a serious debate on certain policy issues because there's no shared epistemological framework. We're debating what is true and what isn't, and we spend all our time on that, and we never get to the actual debate over policy. But again, that's just a broader issue, and it's not addressed by our bill right now.

Coaston: So Donald Trump supported banning TikTok, and now he doesn't. How much harder does that make it for Republicans to vote for this legislation?

Gallagher: So in many ways I was surprised by his statement because a lot of this started with Trump. I mean, he was ahead of the curve when he tried to address the national security problems posed by ByteDance ownership of TikTok. And our bill is an extension of that effort. Obviously his effort ran into a legal buzz saw. We tried to learn from that and draft the bill in a way where it would survive a legal challenge and was on the strongest constitutional grounds. The bill is not trying to shut TikTok down and then force all its users onto Facebook. So if that's the former president's concern, then this bill should not worry him, because that is not the intent, and that, I don't think, is what would practically happen. And then we had the vote after he made the statement, and we still got 352 votes. I think that just shows that there's serious bipartisan concerns about ByteDance's ownership of TikTok, and either this administration or the next administration, which could be the Trump administration, is going to have to address it.

After the interview, I followed up with Mr. Gallagher via email on a few points. These have also been edited for length and clarity.

Coaston: Conservatives also used to be pretty leery of government control and intervention. The approach of many conservatives to TikTok feels to me like “government knows best” and “government will call the shots.” Did conservatives change their way of thinking, or is China just scaring the hell out of them?

Gallagher: There’s a clear precedent of the government protecting Americans from national security threats posed by foreign-adversary-controlled applications and preventing our foreign adversaries from influencing the American airwaves. For a century, the Federal Communications Commission has blocked concentrated foreign ownership of radio and television assets on national security grounds, and in 2020, CFIUS (the Committee on Foreign Investment in the United States) forced a divestment of the app Grindr, citing national security concerns stemming from its Chinese ownership.

Coaston: Clearly, there are a lot of younger people who would be upset if a divestment didn’t work and TikTok no longer operated in the United States. How do you think about the politics of that?

Gallagher: Fortunately for the kids, this bill presents a great opportunity for ByteDance to divest of TikTok and continue operating in the United States. This decision is squarely in TikTok’s hands.

The Times is committed to publishing a diversity of letters to the editor. We’d like to hear what you think about this or any of our articles. Here are some tips. And here’s our email: letters@nytimes.com.

Follow the New York Times Opinion section on Facebook, Instagram, TikTok, WhatsApp, X and Threads.

Jane Coaston was the host of Opinion’s podcast “The Argument.” Previously, she reported on conservative politics, the G.O.P. and the rise of the right. She also co-hosted the podcast “The Weeds.”

@janecoaston

‘Thunder Run’: Behind Lawmakers’ Secretive Push to Pass the TikTok Bill

A tiny group of lawmakers huddled in private about a year ago, aiming to keep the discussions away from TikTok lobbyists while bulletproofing a bill that could ban the app.



Listen to this article • 11:06 min [Learn more](#)



By Sapna Maheshwari, David McCabe and Cecilia Kang

Sapna Maheshwari reports on TikTok. David McCabe and Cecilia Kang cover tech policy.

April 24, 2024

Just over a year ago, lawmakers displayed a rare show of bipartisanship when they grilled Shou Chew, TikTok’s chief executive, about the video app’s ties to China. Their harsh questioning suggested that Washington was gearing up to force the company to sever ties with its Chinese owner — or even ban the app.

Then came mostly silence. Little emerged from the House committee that held the hearing, and a proposal to enable the administration to force a sale or ban TikTok fizzled in the Senate.

But behind the scenes, a tiny group of lawmakers began plotting a secretive effort that culminated on Wednesday, when President Biden signed a bill that forces TikTok to be sold by its Chinese owner, ByteDance, or risk being banned. The measure, which the Senate passed late Tuesday, upends the future of an app that claims 170 million users in the United States and that touches virtually every aspect of American life.

For nearly a year, lawmakers and some of their aides worked to write a version of the bill, concealing their efforts to avoid setting off TikTok's lobbying might. To bulletproof the bill from expected legal challenges and persuade uncertain lawmakers, the group worked with the Justice Department and White House.

And the last stage — a race to the president's desk that led some aides to nickname the bill the “Thunder Run” — played out in seven weeks from when it was publicly introduced, remarkably fast for Washington.

“You don't get many opportunities like this on a major issue,” said Representative Steve Scalise of Louisiana, the Republican majority leader. He was one of 15 lawmakers, aides and officials directly involved in shaping and passing the bill who were interviewed for this article.



Representative Steve Scalise, the Republican majority leader, pushed for a bipartisan effort to address security concerns over TikTok. Jason Andrew for The New York Times

“This fight’s been going on for years,” Mr. Scalise said. “We learned a lot from each step, and we wanted to make sure we had strong legal standing and a strong bipartisan coalition to do this.”

Their success contrasts with the stumbles by other lawmakers and American officials, starting during the Trump administration, to address national security concerns about TikTok. They say the Chinese government could lean on ByteDance to obtain sensitive U.S. user data or influence content on the app to serve Beijing’s interests, including interfering in American elections.

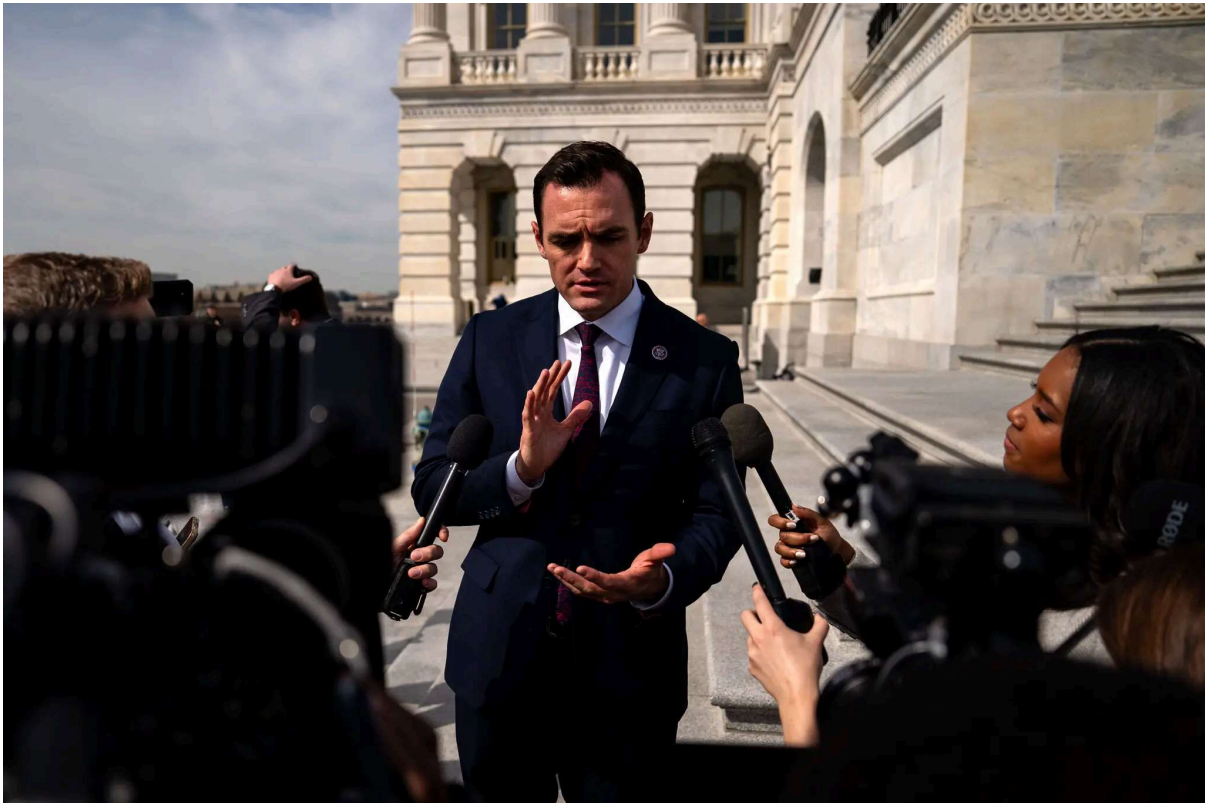
TikTok has pushed back against those accusations, saying that the Chinese government plays no role in the company and that it has taken steps and spent billions of dollars to address the concerns. It has also fought back aggressively in the courts against previous actions by federal and state governments.

But the strategy employed by the lawmakers in recent weeks caught TikTok flat-footed. And while the app is unlikely to disappear from Americans’ phones as next steps are worked out, the measure stands out as the first time a U.S. president has signed a bill that could result in a wide ban of a foreign app.

In a statement, Alex Haurek, a TikTok spokesman, said the bill “was crafted in secret, rushed through the House and ultimately passed as part of a larger, must-pass bill exactly because it is a ban that Americans will find objectionable.”

He added that it was “sadly ironic that Congress would pass a law trampling 170 million Americans’ right to free expression as part of a package they say is aimed at advancing freedom around the world.”

From Tiny Huddle to Big Majority



Representative Mike Gallagher speaking to reporters on the day the House voted to pass the TikTok bill. Kent Nishimura for The New York Times

The effort around a TikTok bill began with Mr. Scalise, who met with Representative Cathy McMorris Rodgers, a Republican from Washington, in March last year about their desire to see a measure that took on the app.

They began talking with other Republican lawmakers and aides across several committees about a new bill. By August, they had decided to shepherd a potential bill through a House committee focused on China, the Select Committee on the Chinese Communist Party, led by Representatives Mike Gallagher, a Wisconsin Republican and its chairman, and Raja Krishnamoorthi, an Illinois Democrat.

The bipartisan committee swiftly embraced the effort. “What we recognized was that there were so many different approaches and the technical issues were so complex,” Mr. Krishnamoorthi said.

So the committee hatched a strategy: Win the support of Democrats, the White House and the Justice Department for a new bill.

Its efforts got a lift after lawmakers including Mr. Gallagher accused TikTok of intentionally pushing pro-Palestinian and anti-Israel content to its users last year. Mr. Krishnamoorthi and others said the Israel-Gaza conflict stoked lawmakers' appetites to regulate the app.

In November, the group, which then numbered fewer than 20 key people, brought in officials from the Justice Department, including Lisa Monaco, the deputy attorney general, and staff from the National Security Council to help secure the Biden administration's support for a new bill.

For years, the administration had weighed a proposal by TikTok, called Project Texas, that aimed to keep sensitive U.S. user data separate from the rest of the company's operations. The Justice Department and National Security Council officials agreed to support the new bill partly because they saw Project Texas as inadequate to handle national security concerns involving TikTok, two administration officials said.

In conversations with lawmakers, White House officials emphasized that they wanted ByteDance to sell TikTok rather than impose a ban, partly because of the app's popularity with Americans, three people involved in the process said.

The Justice Department and Ms. Monaco provided guidance on how to write the bill so it could withstand legal challenges. TikTok previously fended off efforts to ban it by citing the First Amendment rights of its users. The officials explained how to word the bill to defend against those claims, citing national security.

With the administration's support in hand, the group quietly solicited more supporters in the House. The Justice Department joined members of the Office of the Director of National Intelligence and F.B.I. to brief House committees on the threats posed by TikTok's Chinese ownership. The briefings were later delivered in the Senate.

Ms. Monaco also met individually with lawmakers, warning them that TikTok could be used to disrupt U.S. elections.

“She built out a powerful case, and we agreed that not only was data gathering taking place, she shared that you have 170 million American that were vulnerable to propaganda,” Senator Mark Warner, Democrat of Virginia, said of a meeting with Ms. Monaco in Munich in February.

On March 5, Mr. Gallagher and Mr. Krishnamoorthi announced the bill and named around 50 House members who endorsed it. The Energy and Commerce Committee, which is led by Ms. McMorris Rodgers, took the bill up that week.

TikTok, which had been negotiating with U.S. officials over its Project Texas plan, was caught off guard. It quickly sent information to members of the Energy and Commerce Committee outlining TikTok’s economic contributions in their districts, according to documents viewed by The New York Times. It also used a pop-up message on its app to urge users to call legislators to oppose a ban.

But when hundreds of calls flooded into some lawmakers’ offices, including from callers who sounded like minors, some of the lawmakers felt the bill was being misrepresented.

“It transformed a lot of lean yeses into hell yeses at that point,” Mr. Krishnamoorthi said.

Former President Donald J. Trump, the presumptive Republican presidential nominee, voiced opposition to the bill, causing panic. But Mr. Scalise said he had urged Mr. Trump to reconsider, and a vote proceeded.

Two days after the bill was unveiled, Ms. McMorris Rodgers’s committee voted 50 to 0 to advance it to the full House, where it passed the next week by 352 to 65.

There were tears of joy in Mr. Krishnamoorthi’s office, two people said. Mr. Gallagher’s staff members celebrated with a cookie cake sent by Mr. Scalise, one of his signature rewards for successful legislation.



Members of Mr. Gallagher's staff holding a cookie cake sent from the office of Mr. Scalise to celebrate the TikTok bill's passage in the House last month. Kent Nishimura for The New York Times

A Less Certain Future

Even with the bill's swift passage in the House, its future in the Senate was uncertain. Some senators, including powerful committee chairs like Maria Cantwell, a Democrat of Washington, and Mr. Warner, considered changes to the bill in a process that could significantly slow it down.

The House bill gave ByteDance six months to sell TikTok. Senators wanted to extend the timeline and detail the government's national security concerns about TikTok in the bill, to make it clear to courts how it justified the measure.

As the Senate worked on the bill, TikTok contacted lawmakers' offices and spent at least \$3 million in ads to defend itself. It blanketed the airwaves in key states with commercials depicting how users — like nuns and ranchers — make a living and build communities through the app.

TikTok also had support from conservative groups like Club for Growth and the Cato Institute, both backed by Jeffrey Yass, a prominent investor in the app, and liberal organizations like the American Civil Liberties Union, which said the bill would violate Americans' First Amendment rights.

A Club for Growth spokesman said Mr. Yass “never requested Club to take a position or action on his behalf.”

Some deep-pocketed groups on the right mobilized to support the bill. One was the American Parents Coalition, backed by Leonard Leo, a conservative activist, which ran an ad campaign called “TikTok Is Poison” in March. A spokesman for Mr. Leo said he was “proud to support” the group’s efforts.

Some in Silicon Valley also spoke out in favor of the bill, including Vinod Khosla, a venture capitalist, and Jacob Helberg, a senior policy adviser to Palantir’s chief executive.

Bijan Koohmaraie, a counsel in Mr. Scalise’s office who helped drive the bill, said a main reason to keep the process secret for so long had been to keep lobbyists away.

“No company had any influence or was helping draft this bill on the outside,” he said.

A New Opportunity

As the bill sat in the Senate, a new opportunity presented itself. The House speaker, Mike Johnson, announced an attempt last week to pass foreign aid for countries including Ukraine. To ensure he had the votes, Mr. Johnson took the unusual step of attaching a package of bills popular with Republicans, including the TikTok measure.

Senators scrambled now that the House had forced their hand. Ms. Cantwell’s office asked the House for multiple edits to the measure, a person with knowledge of the matter said.

House lawmakers made just one change the Senate wanted. The version of the bill in the aid package extended the deadline for a TikTok sale to nine months from six months. The president can add another 90 days if ByteDance has made progress toward selling TikTok.

“The most important thing is to have enough time to effect a sale,” Ms. Cantwell said.

The change was enough. Late Tuesday, the Senate passed the bill overwhelmingly, 79 to 18. On Wednesday morning, Mr. Biden signed it into law.

***A correction was made on April 24, 2024:** An earlier version of a picture caption with this article misidentified the date of the photo. It was last year, not last month.*

When we learn of a mistake, we acknowledge it with a correction. If you spot an error, please let us know at nytnews@nytimes.com. [Learn more](#)

Sapna Maheshwari reports on TikTok, technology and emerging media companies. She has been a business reporter for more than a decade. Contact her at sapna@nytimes.com. [More about Sapna Maheshwari](#)

David McCabe covers tech policy. He joined The Times from Axios in 2019. [More about David McCabe](#)

Cecilia Kang reports on technology and regulatory policy and is based in Washington D.C. She has written about technology for over two decades. [More about Cecilia Kang](#)

Home > ... > Secretary Antony J. Blinken At McCain Institute's 2...

Secretary Antony J. Blinken At McCain Institute's 2024 Sedona Forum Keynote Conversation with Senator Mitt Romney

REMARKS

ANTHONY J. BLINKEN, SECRETARY OF STATE
SEDONA, ARIZONA

MAY 3, 2024

SENATOR ROMNEY: I don't know who gets to go off first, but I'm going to do that, because I get to ask the questions. I'm not the questioner, usually. Usually I'm the person trying to give answers, all right? Have you ever watched Mr. Roger's Neighborhood? There's a little train and there's the little king, and he – the king is always right – “Right as usual, King Friday.” My kids say, “Right as usual, King Romney.” I mean, because I'm – (laughter) – I'm always out there with the answers.

So I – tonight I'm supposed to ask the questions, which I will do. But I want to begin by saying thank you to Cindy McCain for hosting us and bringing this extraordinary group together. Thank you to the Navalny family and for your beautiful words – extraordinary. Thank you so very much for your inspiration. It is touching and powerful. Thank you to the McCain Institute. Thank you to David Axelrod. I have mixed emotions about David Axelrod. (Laughter.)

I appreciate the Secretary of State and his leadership very much. And we're fortunate to have a Secretary of State who's a thoughtful, perceptive, intellectually curious, devoted person; dedicated, determined, indefatigable, who has traveled the world time and time again – not a person of bombast, but a person who listens and is soft-spoken. We are very fortunate to have a man of the kind of quality, experience, and character as our current Secretary of State, Secretary Antony Blinken. Thank you. (Applause.)

So because I'm not noted for my questions – and frankly, my answers aren't much better – (laughter) – but I'm going to ask a few questions, but if there's a little time, I might turn to you to ask, if there are questions. I'm going to just sort of go topic area by topic area. I'm going to start with the Secretary's most recent trip to the Middle East and then turn to Ukraine, and then finally to China. And so if there's someone who has a question on one of those topics, or – I'll take a breath, and you can – and please ask questions that are interesting to you, but also, you might think, to the entire audience. (Laughter.)

First, I'm going to say up top, with regards to the trip to the Middle East, give us the lowdown, give us the rundown. What is happening there? What's happening among the Israeli people? What are – what is Bibi Netanyahu thinking? What's happening with Hamas? What kind of a deal has been put on the table? What's – what is – the people and the leadership in Qatar – see, I can get all my questions out. (Laughter.) I mean, give us a full lay of the land, and then we can sort of probe areas of interest.

SECRETARY BLINKEN: Mitt, thank you. And before trying to tackle that multi-part question – (laughter) – actually, it sounds like —

SENATOR ROMNEY: It's – it's just the lay of the land.

SECRETARY BLINKEN: It sounds like the reporters in my pool, who manage to get in five questions for one.

First, let me say how wonderful it is to be here and to be with a truly remarkable group of people. I think there's a common denominator in this room, and it's epitomized by John McCain, it's epitomized by Mitt Romney, but everyone in this room is for an engaged America. Everyone in this room believes that our engagement, our leadership matters, makes a difference. And that commitment is more important than it's ever been. That's what I'm seeing and feeling around the world.

Now, it may be that years from now people come back here and look at this group, and it's the La Brea Tar Pits of internationalists and institutionalists. (Laughter.) But we're fighting to make sure that's not the case, and no one has fought harder than the gentleman sitting to my right.

Now, Mitt, I was going to say thank you for reading the lines that I wrote – (laughter) – appreciate that. But I think you all know – the country all knows – Mitt Romney is a man of extraordinary principle, married to extraordinary pragmatism. It's a rare combination, and I've gotten to see that up close these last few years since you've been in the Senate. But for me, it's an honor to share the stage with you. So thank you. (Applause.)

SENATOR ROMNEY: Thank you.

SECRETARY BLINKEN: And to the entire McCain family, starting with Cindy – following in the footsteps of John McCain – there too I have gotten to work with Cindy these last few years. You are doing what is maybe the greatest calling anyone could have, which is trying to make sure that parents can put food on the table for their kids. And when it comes down to it, nothing matters more than that. So to you, to the entire family that remains so engaged, it's wonderful to be here and to share this evening with you.

Now, I have to tell you – and maybe the Middle East is actually a – it's a perfect segue to the Middle East. But let me just say quickly, before we were coming out here, we were listening, Dasha, we were listening to you, and the senator and I had the same reaction: Let's go in the other direction, because we don't want to follow Dasha. (Laughter.) Thank you for your extraordinary profile in dignity and in courage. And I can only imagine how proud your dad would be of you. (Applause.)

So when I'm asked how it's going, and the Middle East is usually the first thing I'm asked about, I actually tend to quote John McCain. John McCain used to say, "It's always darkest before it goes completely black." (Laughter.) So – and I thank you, Cindy, for letting me borrow that.

But now to get serious for a minute, so in this moment, the best thing that can happen would be for the agreement that's on the table that's being considered by Hamas – to have a ceasefire, the release of hostages, the possibility of really surging humanitarian assistance to people who so desperately need it – that's what we're focused on. And as I was talking to various colleagues this morning – and I see one of my closest colleagues, John Finer, the deputy national security advisor, here – we await a response from Hamas. We await to see whether, in effect, they can take yes for an answer on the ceasefire and release of hostages. And the reality in this moment is the only thing standing between the people of Gaza and a ceasefire is Hamas. So we look to see what they will do.

In the meantime, even as we're doing that, we are working every single day, the President's working every single day, to make sure that we are doing what we can so that the people in Gaza who are caught in a crossfire of Hamas's making get the help, the assistance, the support they need. And we're doing that with partners like the World Food Program; and of course, we're working with many other governments, we're working with Israel.

I was just there, as you said, and I got to see firsthand some of the progress that's been made in recent weeks in actually getting assistance to people who need it. Progress is real; it's still not enough. And we are trying to make sure that in everything we do, we're supporting those efforts.

If you step back, I think we've seen a few things in the last few weeks – some incredibly promising, others incredibly daunting. And to start with the daunting, we now have the Israelis and Palestinians, two absolutely traumatized societies, and when this conflict ends, building back from that trauma is going to be an extraordinary task.

We also see in all directions – and I think we're seeing this not only in the region, we're seeing it around the world; to some extent we're seeing it in our own country – maybe the biggest poison that we have to fight constantly, and that is dehumanization, the inability to see the humanity in the other. And when that happens, hearts get hardened, and everything becomes so much more difficult.

So the other great task that I think we're going to have when we get through this is to build back that sense of common humanity. And I hope we can do that amongst ourselves as well. But there's also some promise. There's promise in that one of the things we've been working on for a long time, with the President's leadership over many months, is seeking to normalize relations between Saudi Arabia and Israel. And for Israel, this would be the realization of something that it's sought from day one of its existence: normal relations with other countries in the region.

This is something we were working on before October 7th. In fact, I was due to go to Israel and Saudi Arabia on October 10th to work on this, and in particular to work on the Palestinian piece of the puzzle, because for us, for the Saudis, if we're able to move forward on normalization, it has to include also moving forward on the aspirations of the Palestinian people.

So I think there's an equation that you can see, a different path that countries in the region can be on and really want to be on, which is a path of integration, a path where Israel's relations with its neighbors are normalized; a path where Israel's security is actually looked out for, including by its neighbors; a path where Palestinians achieve their political rights; and a path in which the biggest threat to Israel, to most of the countries in the region, and a threat that we share, Iran, is actually isolated.

Now, whether we can move from the moment that we're in to actually start to travel down that path, that's going to be a big challenge. But you can see it, and it's something that the President is determined to try to pursue if we have the opportunity to do it.

One other thing on this. We saw something related that was quite extraordinary about two weeks ago. Iran engaged in an unprecedented attack on Israel, the first direct attack from Iran to Israel. And some people said, well, it was designed so it wouldn't do much damage, carefully calibrated. Nothing of the sort. More than 300 projectiles launched at Israel, including more than a hundred ballistic missiles. John and I were in the Situation Room watching this unfold.

It's because Israel had very effective defenses – but also because the President, the United States, managed to rally on short notice a collection of countries to help – that damage was not done. And that also shows something in embryonic form: the possibilities that Israel has for, again, being integrated, a regional security architecture that can actually, I think, keep the peace effectively for years to come.

So that's where we want to go. But getting from here to there, of course, requires that the war in Gaza come to an end. And right now, the quickest path to that happening would be through this ceasefire and hostage deal.

SENATOR ROMNEY: I think a number of folks, myself included, have wondered why Hamas has not agreed to other proposals with regards to a ceasefire. What are we misunderstanding? What is their calculation? What are they – why are they hesitating? This – I mean, we read about what's being proposed. It sounds like a no-brainer. But they must have a different calculation. What is going through their head? What – I mean, they want to be just martyrs? Is that – I mean, what is it that they hope to carry out, and why have they not just jumped on this, saying, oh, yeah, this is fantastic?

SECRETARY BLINKEN: One of the challenges we have, of course, is that the leaders of Hamas that we're indirectly engaged with through the Qataris, through the Egyptians, are of course living outside of Gaza, living in Qatar or living in Türkiye, other places, and the ultimate decision makers are the folks who are actually in Gaza itself with whom none of us have direct contact. So trying to understand what they're thinking is a challenge. Now, we have some sense of it, but it's not – it's far from perfect. And there are different theories about what's actually motivating their decisions in this time. It's something we – we're constantly trying to get at.

But I can't give you a definitive answer, and I think we'll see, depending on what they actually do in this moment, whether in fact the Palestinian people whom they purport to represent – if that's actually true; because if it is true, then taking the ceasefire should be a no-brainer, as you said. But maybe something else is going on, and we'll have a better picture of that in the coming days.

SENATOR ROMNEY: Tell us about Bibi Netanyahu and what his – what his position of power is, how he's seen among the Israeli people, what the level of commitment is in Israel for them to go into Rafah, to continue this effort. Where is he? If this – well, I'm not – I'm going to take the if out. I was going to go back to the ceasefire. But what's his political posture now in Israel?

SECRETARY BLINKEN: Well, I think, as everyone knows, this is a complicated government. It's a balancing act when you have a coalition. And if you're just looking at the politics of it, that's something that he has to factor in.

But here's what I'd say generally about this. Irrespective of what you think of the prime minister, the government, what's important to understand is that much of what he's doing is not simply a reflection of his politics or his policies; it's actually a reflection of where a large majority of Israelis are in this moment. And I think it's important to understand that if we're really going to be able to meet this challenge. That's at least my observation.

I've now been there seven times since October 7th, and you get a chance to get a feel for what's going on in the society itself. And as I said at the start, you have a traumatized society, just as you have traumatized Palestinians. And breaking through that trauma in real time is an extraordinary challenge. But it's I think very important that we, as the United States, as Israel's friend, try to share what we think is not only in our interest but also what's in their interest. And when it comes to Rafah – Mitt, you mentioned that a moment ago – look, our position is clear. The President's been clear on this. Absent a credible plan to genuinely protect civilians who are in harm's way – and keep in mind there are now 1.4 million or so people in Rafah, many of them displaced from the north – absent such a plan, we can't support a major military operation going into Rafah because the damage it would do is beyond what's acceptable.

So we haven't seen such a plan yet, but right now, as I said, the focus is intensely on seeing if we can't get this agreement because that would be a way of, I think, moving things in a different direction.

SENATOR ROMNEY: You may not want to answer this question, but that is – the President sort of dipped his toe into the criticism of Israel and the way they've conducted the war so far, saying we're not entirely happy with how this has been carried out. What would our administration have done differently? What is our specific criticism, and what guidance will that provide for what they do going forward?

SECRETARY BLINKEN: Well, let's start with the – in a sense, the obvious that seems to have been forgotten, or almost erased from the conversation, which is October 7th itself. And it's extraordinary how quickly the world moved on from that.

It's also extraordinary the extent to which Hamas isn't even part of the conversation. And I think that's worth a moment of reflection, too. And so we've said from the start, and the President has been committed from the start, to the proposition that Israel not only has a right to defend itself, not only has a right to try to make sure October 7th never happens again, it has an obligation. And so that's something that we have supported from day one.

But we've also said – also from day one – how it does it matters. And here, the damage that's been done to so many innocent children, women, and men – again, in this crossfire of Hamas's making – has to be something that we focus on, as it has been from day one, trying to make sure that the assistance gets to those who need it, trying to make sure that civilians are protected to the greatest extent possible.

Now, everyone here knows that this is a – almost a unique challenge because when you have an enemy, a terrorist group like Hamas that embeds itself with the civilian population in ways that we really haven't seen before, and that is hiding in and under mosques, schools, apartment buildings, it's an incredibly tall order. But even so, even so, I think where we've been pushing our friends – again, from the very start – is to do as much as possible, and to do more, to look out for civilians, and to make sure that those who need the help get it.

SENATOR ROMNEY: Why has the PR been so awful? I know that's not your area of expertise, but you have to have some thoughts on that, which is, I mean, as you've said, why has Hamas disappeared in terms of public perception? An offer is on the table to have a ceasefire, and yet the world is screaming about Israel. It's like, why are they not screaming about Hamas? Accept the ceasefire and bring home the hostages. Instead, it's all the other way around. I mean, typically the Israelis are good at PR. What's happened here? How have they – how have they/ and we/ been so ineffective at communicating the realities there and our point of view?

SECRETARY BLINKEN: Look, I mean, there are two things. One is that, look, there is an inescapable reality, and that is the inescapable reality of people who have and continue to suffer grievously in Gaza. And that's real and we have to – have to – be focused on that and attentive to that.

At the same time, how this narrative has evolved, yeah, it's a great question. I don't have a good answer to that. One can speculate about what some of the causes might be. I don't know. I can tell you this – and we were talking about this a little bit over dinner with Cindy. I think in my time in Washington, which is a little bit over 30 years, the single biggest change has been in the information environment. And when I started out in the early 1990s, everyone did the same thing. You woke up in the morning, you opened the door of your apartment or your house, you picked up a hard copy of *The New York Times*, *The Washington Post*, *The Wall Street Journal*. And then if you had a television in your office, you turned it on at 6:30 or 7 o'clock and watched the national network news.

Now, of course, we are on an intravenous feed of information with new impulses, inputs every millisecond. And of course, the way this has played out on social media has dominated the narrative. And you have a social media ecosystem environment in which context, history, facts get lost, and the emotion, the impact of images dominates. And we can't – we can't discount that, but I think it also has a very, very, very challenging effect on the narrative.

The President had also spoken about our commitment to a two-state solution, and a number of people have said to me that's impossible. And Bibi Netanyahu has basically said that's impossible. Is it possible to have a two-state solution? What kind of – I mean, I know that's far from where we are right now. It's like a whole different realm. But is that essential to, if you will, beginning normalization relations with Saudi Arabia and with others to say, hey, here's a vision, here's some steps we might get to? Is it possible, and what would that look like?

SECRETARY BLINKEN: So for me and the President, the answer is yes. And you can say that's – especially in this moment – naïve, impossible. But I think that it is an imperative. And let me put it this way. First, we were talking about normalization with Saudi Arabia. I've sat with MBS multiple times, the crown prince, and he's made clear that he wants to pursue normalization and he'd like to do it as soon as possible – if we can conclude the agreements that we're trying to reach between the United States and Saudi Arabia. But then two requirements: one, calm in Gaza; two, a credible pathway to a Palestinian state. This is what people in the region need to see if they're going to fully get behind normalized relations between the remaining Arab countries and Israel. And it's also the right thing for the Palestinians. So there's that.

But the other, I think, more fundamental question is this. You've got 5 million Palestinians living between the West Bank and Gaza. You've got about 7 million Jews. The Palestinians aren't going anywhere; the Jews aren't going anywhere. There has to be an accommodation. Now, I think that some believe that the status quo that prevailed before October 7th – fine, let's live that way. And that worked brilliantly until it failed catastrophically.

So at some point, I believe there has to be a step back. And everyone's going to have to ask themselves questions about what do we want the future to be. And the future that I talked about a few minutes ago, where Israel finally realizes what it has sought from day one – to be accepted in the region, to be part of the neighborhood – that's achievable. It's there, but it also requires a resolution to the Palestinian question. And I believe that there can be a Palestinian state with the necessary security guarantees for Israel. And to some extent, I think you have Israelis who would like to get to real separation. Well, that is one way to do it. And then who knows what happens in the following years.

But of course, as we say this, we are absolutely committed to Israel's security. And Israel cannot and will not accept a Hamastan coming together next door. But I'm convinced that there are ways to put the Palestinians on a pathway to a state that demonstrate that the state will not be what Israelis might fear, and I think can lead to a much better future than we have.

Look, everyone in this room knows there's a long story here. We were talking about TikTok. Not a story you hear on TikTok. You had – to oversimplify, after the creation of the state of Israel you had decades of basically Arab rejection. That went away with Egypt and Jordan making peace, and others following. Then you had some decades, in effect, of Palestinian rejection, because deals were put on the table – Camp David, Ehud Olmert, others – that would have given Palestinians 95, 96, 97 percent of what they sought, but they were not able to get to yes. But I think the last decade or so has been one in which maybe Israelis became comfortable with that status quo. And as I say, I just don't think it's sustainable.

SENATOR ROMNEY: Yeah. Yeah. Anyone else, topic? Israel, Middle East? Yes, sir.

QUESTION: (Inaudible.)

SENATOR ROMNEY: You've got to be real loud. And I'm going to repeat it, but it's got to be short, too.

QUESTION: All right, it's very short. You talked about Israel and Palestine, Saudi Arabia being such a key U.S. ally there. What do you see with China, Taiwan, India, Japan kind of doing the same (inaudible)? What efforts (inaudible)? What are the complications that you're running into trying to overcome the China threat and the Russian threat to European allies?

SECRETARY BLINKEN: Maybe that's a great segue. Did we need a segue?

SENATOR ROMNEY: There you go, go ahead. Yeah, please.

SECRETARY BLINKEN: All right. Well, just a few things to say here. First, with China, just before we were in the Middle East we were in China. And about a little less than a year ago, I took a trip at a time when we had been very disengaged. And I think that one of the things that President Biden believes is that we have an obligation to try to manage this relationship responsibly. We're in an intense competition with China, and of course, for Americans there's nothing wrong with competition as long as it's fair. Hopefully it actually brings out the best in us. But it is a real competition.

But we also have a profound interest in making sure that competition doesn't veer into conflict, and that actually starts with engagement. And so we really began a process of re-engagement with our eyes wide open, and a number of my colleagues followed. And then, of course, most important, President Biden and President Xi met at the end of the year in San Francisco on the margins of the APEC meeting.

And what we've tried to do, first and foremost, is to re-establish regular dialogue at all levels. One of the most important pieces of this was re-establishing military-to-military communications, because the quickest way to get into an unintended conflict is not to have those conversations happen. That's been fully restored. We look for areas where we might actually cooperate where it happens to be in our mutual interest to do that – and I'll come back to this in a second because we found a couple. But mostly, it's so important because you want to be able to be extremely clear, extremely direct, extremely explicit about your differences and your intentions. And we have a world of differences, but it's better to be talking about them directly than it is to remain disengaged.

In No Labels Call, Josh Gottheimer, Mike Lawler, and University Trustees Agree: FBI Should Investigate Campus Protests

 theintercept.com/2024/05/04/josh-gottheimer-mike-lawler-campus-protests

May 4, 2024

During a call hosted by the centrist political group No Labels, Reps. Josh Gottheimer, D-N.J., and Mike Lawler, R-N.Y., spoke with close to 300 attendees, including trustees from several universities, about how Congress could help crack down further on student protesters — and how the FBI could get more involved.

No Labels promoted the Wednesday event as a “special Zoom call” with “the leading voices in their parties” opposing student protests against the war in Gaza, which spread to more than 150 campuses in the last two weeks.

The bipartisan pair praised the responses of universities that have called on police to violently quell protests and promised that Congress would be doing more to investigate the student movements, according to a recording of the meeting obtained by The Intercept. The lawmakers and university board of trustee members repeatedly claimed that nefarious outside actors are funding and organizing the encampments on university campuses.

Gottheimer said that he had been in touch with officials from the Federal Bureau of Investigation about campus protests. “Based on my conversations with the FBI — there’s activity I can’t get into, you know, given my committee responsibilities, I can’t get into more specifics — but I can just say that I think people are well aware this is an issue,” said Gottheimer, who is on the House Intelligence Committee.

“I can’t speak for the local FBI field offices, but it’s got to be all hands on deck,” he added. “I believe following the money is the key. Gotta follow the money. A lot of these universities are not transparent at all, remotely, about where the money comes from, you know, they just, they want it — and that has to be a big part of this.”

This week, House Republicans said they would investigate federal funding for universities that held campus protests. House Speaker Mike Johnson, R-La., announced the plans on Tuesday alongside the chairs of six congressional committees.

Gottheimer and Lawler have been at the forefront of congressional efforts to defend Israel amid its brutal war on Gaza. They led bipartisan efforts to silence criticism of Israel and to protect Israel from being held accountable for using the billions of dollars it receives from the United States in violation of international law.

Gottheimer, Lawler, and No Labels did not respond to requests for comment.

Among the most prominent themes of the discussion were getting the FBI more involved in investigating American college campuses, and fears of outside agitators stoking the anti-war protests. New York University Chair Emeritus and Executive Vice Chair Bill Berkley, whose campus this week welcomed police to arrest over a dozen students, claimed that a New York City-based Palestine solidarity group had been very involved in leading protest efforts in the city and suggested that the feds should investigate.

Berkley claimed that “we have deciphered messages” that showed the group directing people to the encampment at Columbia. He also suggested that, because many of the tents at campus protests were the same, the demonstrations had been orchestrated externally. (Many prominent critics of the protest, including New York City Mayor Eric Adams, have repeated that claim. As the New York City outlet Hell Gate and others have pointed out, the tents are sold for \$15 at Five Below and around \$30 at Amazon and Walmart. “My God... looks like what we’ve got on our hands is a classic case of college students buying something cheap and disposable,” wrote Hell Gate.)

Berkley then asked why the FBI hadn’t yet taken action against the demonstrations. “And, by the way, the FBI and the terrorist monitoring groups know this — why haven’t we seen any action by the federal government?” He did not respond to requests for comment.

“You’re seeing how these kids are being manipulated by certain groups or entities or countries to foment hate on their behalf and really create a hostile environment here in the U.S.”

Lawler, who co-sponsored a recent bill to ban TikTok, repeated Berkley’s claims about external organizers and said that was the type of thing that inspired Congress’s efforts to ban the app. “I don’t think there’s any question that there has been a coordinated effort off these college campuses, and that you have outside paid agitators and activists,” Lawler said. “It also highlights exactly why we included the TikTok bill in the foreign supplemental aid package because you’re seeing how these kids are being manipulated by certain groups or entities or countries to foment hate on their behalf and really create a hostile environment here in the U.S.”

Lawler added that he would look into domestic groups funding protests. Gottheimer, for his part, said demonstrations at Columbia were “potentially” led by outsiders and repeated his frequent claim that the protesters support Hamas.

Andrew Bursky, the board chair of Washington University in St. Louis, Missouri, said America’s tradition of campus protests was “a positive thing,” but that there’s a “clear dark line” between allowing free speech and condoning antisemitism. “And I think you guys in Congress have darkened that line today with this piece of legislation,” he added. Bursky did not specify what legislation he was referring to, but earlier that day, the House of Representatives passed a Republican-led bill that expanded the definition of antisemitism.



Interview With Former U.S. Director of National Intelligence John Ratcliffe; Interview With Rep. Elise Stefanik (R-NY); Interview With Former New York City Police Commissioner Raymond Kelly;...

Fox News Network

May 05, 2024 8:00 AM

Copyright 2024 Fox News Network LLC All Rights Reserved

Author: Maria Bartiromo

Section: NEWS, International

Print Edition: Fox News

Length: 7038 words

Body

MARIA BARTIROMO, FOX NEWS ANCHOR: Good Sunday morning, everyone. Thanks so much for joining us this morning. Welcome to "Sunday Morning Futures." I'm Maria Bartiromo.

Today: saboteurs in America piling on. Antisemitism rages in America, in some cases by outside educators inside the country. But Joe Biden waits 10 days to speak out against it, then claims Islamophobia is just as big a problem right now.

(BEGIN VIDEO CLIP)

JOE BIDEN, PRESIDENT OF THE UNITED STATES: There should be no place on any campus, no place in America for antisemitism or threats of violence against Jewish students. There is no place for hate speech or violence of any kind, whether it's antisemitism, Islamophobia, or discrimination against Arab Americans or Palestinian-Americans.

It's simply wrong.

(END VIDEO CLIP)

BARTIROMO: Coming up, the woman who first exposed the antisemitism on college campuses, New York Congresswoman Elise Stefanik on federal funding of colleges in the future and who the real adjudicators are today.

Then: As American declines, prosecutors target one man, President Donald Trump on trial, efforts to muddy up 45 with salacious headlines and insider testimony, yet critics say still no evidence of a crime.

Coming up, RNC Co-Chair Lara Trump on her father-in-law's week in a Manhattan courtroom and on new fund-raising and polls showing Trump leading in seven swing states right now.

Plus, former federal prosecutor and Director of National Intelligence John Ratcliffe on a conspiracy to take down Trump, despite the national security risks in plain sight. Coming up: the ultimatum on the table for Hamas: Give up the hostages or face down Israeli forces in Rafah.

Then, former New York City Police Commissioner Ray Kelly on antisemitism, crime and a wide-open border. Can New York be saved?

APP-599

It's all right here, right now on "Sunday Morning Futures."

And we begin this Sunday morning with America's colleges and universities and the impact of the ongoing anti-Israel protests across the country.

Who is funding this, directing it on social media? How many faculty have participated? And what will it mean for schools and students going forward?

Sources saying the coordinated protests are getting direction on social media, and then The Wall Street Journal reported on a Web site called CrimethInc.com, which has become, according to The Journal, a hub anarchists, Antifa activists and radical leftists, telling users -- quote -- "We can wield the most power by occupying the spaces where classes are held and administrators have offices."

This ahead of graduation day upon us across the country, the University of Southern California earlier canceling its graduation ceremony initially set for this Friday, many more schools altering their plans as startling images emerge from top universities.

At George Washington University, protesters defaced George Washington, a statue of the first president, draping the figure in a Palestinian flag with a black-and-white scarf wrapped around its neck. At Stanford University, someone wearing a headband worn by Hamas seen on campus.

At Columbia University, the epicenter of these protests, police stormed the campus Tuesday night, breaking up the anti-Israel encampment and clearing an academic building protesters had seized after the school finally called for law and order to be restored.

New York's finest replaced the Palestinian flag that was raised above Columbia by protesters with the stars and stripes. Thank you to those students and those NYPD.

NYPD sources telling FOX News, of the 282 protesters arrested at Columbia and City College of New York, 134 of them were not affiliated with either school, with New York City Mayor Eric Adams saying outside agitators are to blame for fueling some of the anti-Israel demonstrations.

Meanwhile, President Biden finally spoke out on the anti-Israel protests, saying his administration is not about silencing people who may disagree after 10 days of silence.

(BEGIN VIDEO CLIP)

BIDEN: We are not an authoritarian nation, where we silence people or squash dissent. The American people are heard. In fact, peaceful protest is in the best tradition of how Americans respond to consequential issues.

But, but neither are we a lawless country. We're a civil society, and order must prevail.

(END VIDEO CLIP)

BARTIROMO: Joining me now with more on all of this in this "Sunday Morning Futures" exclusive is House GOP Conference Chair Congresswoman Elise Stefanik, who has been at the forefront of exposing antisemitism on college campuses.

Congresswoman, it's good to see you this morning. Thanks very much for being here.

REP. ELISE STEFANIK (R-NY): Good to be with you, Maria.

BARTIROMO: So, assess the situation today after we did see a fair amount of cleanup at some colleges over the weekend. And I want to get your take on what you want to see happen in terms of federal funding of college universities.

STEFANIK: Well, first of all, Maria, this is a crisis in higher education.

And I want to thank our law enforcement officers. You played the clip of the NYPD. But who has failed are the university presidents. Our law enforcement have done the right thing, bringing security back to these college campuses.

But our university presidents, whether it's Columbia, whether it's Harvard, Penn, whether it's UCLA, Michigan, Yale, the list goes on, they have failed to protect Jewish students. They have also failed to condemn antisemitism.

And let's be honest. These pro-Hamas riots, this is Joe Biden's Democrat Party. Joe Biden not only waited 10 days to condemn. He has been silent since last December with that historic hearing, where you had three Ivy League university presidents fail to condemn the genocide of Jews. Joe Biden waited months to speak out, saying that testimony was unacceptable.

He didn't even say that, actually, in his statement. But he gave it lip service. But this is the radicalized, far left Democrat Party that Joe Biden owns today. It is about lawlessness. It is about anarchy. It is attacking our most precious ally, Israel. And it is hurling antisemitic slurs against Jewish students, as well as physical harassment, physical assault against Jewish students.

So there is a great deal that we are doing in Congress and our oversight. And our legislative solutions will consist of pulling back federal funding, addressing the foreign dollars that are flowing into these institutions and holding these schools accountable.

BARTIROMO: Why haven't the Democrats been more aggressive on this? Chuck Schumer in the Senate, the highest-ranking Jewish person in Congress, hasn't said enough, in my view.

It feels like they're afraid to offend their own base. And Joe Biden, he said -- the first thing he said was, "Those who don't understand what's going on with the Palestinians, I also condemn that," whatever that means.

STEFANIK: Exactly.

This is Joe Biden's Democrat Party today, the pro-Hamas rioters on college campuses, the anarchists. And that's why you're seeing trepidation among Democrats from speaking out, because this is their base. And the reality is, this is why Republicans continue to poll stronger and stronger, because we represent peace and security. We represent standing up for the Constitution.

We represent supporting our ally of Israel, and we strongly condemn antisemitism. There is a reason that House Republicans have led on this, and it's because there has been a void at our universities.

There is a void at the White House, starting with the top of Joe Biden, and there's been a void in Democrat leadership, including Chuck Schumer, which is why we have expanded the investigation and will continue to be good stewards of taxpayer dollars to yank federal funding that is propping up these institutions that are indoctrinating our next generation.

BARTIROMO: Well, I mean, you also have to go back to Schumer's speech on the Senate floor a month ago or so where he called for new elections in Israel, said that Benjamin Netanyahu is not serving the people of Israel anymore.

I mean, this is in the middle of the fight for survival for Benjamin Netanyahu's life and the state of Israel's survival. He's attacking Netanyahu.

STEFANIK: It was unacceptable, and I was proud to respond immediately with fellow House Republican leadership condemning Chuck Schumer's statements.

It is more important than ever that the United States stand strongly with Israel and the duly elected leaders of Israel, as they are fighting for their very existence. And this is why we're very proud to have a strong conference of House Republicans condemning antisemitism and supporting Israel.

That's in stark contrast to Joe Biden, the Democrat Biden campaign, and Chuck Schumer, who have failed to support Israel. And Joe Biden's silence on this is deafening, and he owns these riots because they are a part of the Democrat base. And that's why they're so desperate and trying to morally equivocate from the White House.

BARTIROMO: Congresswoman, tell me about this Antisemitism Awareness Act, which the House voted on Wednesday.

It would mandate the Department of Education to use the international Holocaust Remembrance Alliance Definition of antisemitism. Tell me what this does. How important is this that you all voted on this week?

STEFANIK: This is very important.

This codifies President Trump's executive order. So President Trump doesn't get credit from the mainstream media, but it was President Trump that expanded Title VI protections for Jewish students on college campuses.

And the Biden administration and the Biden Department of Education, they have failed to open up investigations into each of these college campuses that have been egregious and failed to protect Jewish students on those campuses.

So what this legislation does is, that codifies it. It strengthens it legislatively. And we need to continue to hold the Biden administration accountable for their failure to comply with this executive order that's on the books because of President Trump.

BARTIROMO: So who is funding this? I was told that a lot of these groups were getting their direction from social media.

At one point, there was a directive on social media to go and take over buildings where academics take place. And then they went and they took over Hamilton Hall at Columbia. We're hearing a lot that there are another anti -- antagonists that are not connected to the school.

Give us your sense of who's behind it, who's funding it. And how many people are students, versus outside educators?

STEFANIK: These are really important questions, Maria.

So this is a well-organized entity of far left Democrat radical groups domestically. It is well-funded, well-organized. But, in addition, there is a foreign funding piece that is very important that we get to the bottom of, whether it's the foreign funding flowing into these Middle Eastern studies programs at these universities propping up antisemitic professors, as well as propagating antisemitic curriculum.

We need to not allow that foreign funding. And that is going to be an important legislative solution. In addition, any individuals who are part of these pro-Hamas riots or pro-Hamas encampments who are on student visas, those visas need to be revoked and those individuals need to be deported immediately.

And in the case of Columbia, we found from NYPD that over 40 percent of the rioters were unaffiliated with Columbia University, meaning they were neither students, professors, or faculty members. And that just shows the failure of Columbia leadership to deal with this.

They have allowed these outside rioters, these outside far left Democrat pro-Hamas activists to take over their campuses, putting all students at risk, especially Jewish students. So this is why I have called for the resignation of the Columbia president Minouche Shafik.

She negotiated with the terrorists, and that was a recipe for disaster.

BARTIROMO: Look, I know that China also has a role, whether it be the propaganda coming out of TikTok or all the money that China has sent to these institutions. And we never see the Biden administration push back on that.

Is it largely the institutes, the -- that are connected to college institutions, or something else, in terms of China's role?

STEFANIK: Yes, communist China has tried to infiltrate our college campuses through their Confucius Institutes. This is something that Republicans have worked to address to know to not allow Confucius Institutes.

But we're also seeing it in the information warfare space, Maria, that you touched upon TikTok, which is a communist Chinese front to collect data. It's a national security threat. They have promoted antisemitic content on TikTok, and they have suppressed any pro-Israel content on TikTok.

And we know that these radicalized, far leftists utilize TikTok to organize, to get their message out, which is why the ban on TikTok, the requirement that TikTok divest from communist China is so incredibly important. We passed that in the House, and that's a big result that we have been able to deliver.

BARTIROMO: Congresswoman, before you go, let me switch gears and ask you about the Manhattan trial of President Trump right now.

I know that you have issued ethics complaints against the judge. You also want an investigation of Michael Cohen. Tell me what you're doing with regard to that, and how you would you assess this trial right now for Trump?

STEFANIK: This is a political witch-hunt against Joe Biden's opponent, who is Donald Trump, and it's because Democrats cannot win at the ballot box.

The fact that they have a gag order on President Trump in the midst of a general election campaign shows how desperate the Democrats are. You have a corrupt judge in Judge Merchan. Not only did he donate personally to the

Biden campaign, but an immediate member of his family is raising tens of millions of dollars off of the trial itself and attacking Donald Trump.

BARTIROMO: Wow.

STEFANIK: This is the chief online fund-raiser for Adam Schiff, to the tune of nearly \$90 million, Maria.

So this is corrupt to its core, and yet this is -- in the left and the corrupt DOJ, this is apparently what they're doing with lawfare, and we need to stand strong and make sure that this never happens again.

When it comes to the star witness for this political witch-hunt, this is an individual who perjured himself in front of Congress, who is a known liar. And I urge the Department of Justice to continue the criminal contempt against Michael Cohen.

But there is no case here. It is desperation, and it's a desperate form of election interference.

BARTIROMO: Congresswoman, you were in Mar-a-Lago this week. Did President Trump bring up you being his vice presidential candidate?

STEFANIK: Oh, we had a lot of great members there.

What really came out across to me, Maria, was how unified the Republican Party is and how many rising stars we had. There's a lot of names that are in the mix. I'm honored to have my name as one of them in the mix right now.

But it is a true testament to the strength of the Republican Party. You have so many up-and-comers who are working hard every day to save America. And this is really a unified campaign to support President Trump...

BARTIROMO: OK.

STEFANIK: ... who will save this country this November.

BARTIROMO: Congresswoman, it's good to see you this morning. Thanks very much.

STEFANIK: Thanks, Maria.

BARTIROMO: All right, Elise Stefanik joining us this morning in New York.

Quick break, and then: Treasury Secretary Janet Yellen gets political, warning against a second term from former President Trump, while inflation is up nearly 19 percent and growth has fallen to just 1.6 percent on her watch.

(BEGIN VIDEO CLIP)

JANET YELLEN, U.S. TREASURY SECRETARY: Democracy is associated with strong, independent institutions that uphold the rule of law. Winners are not predetermined or subject to arbitrary and unpredictable whims of political leaders.

(END VIDEO CLIP)

BARTIROMO: RNC Co-Chair Lara Trump with reaction, as new polling shows the 45th president leading in seven crucial swing states.

Stay with us.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

DONALD TRUMP, FORMER PRESIDENT OF THE UNITED STATES (R) AND CURRENT U.S. PRESIDENTIAL CANDIDATE: But the one thing that has been interesting about this four years, it shows how bad their policies are. It shows that their policies don't work.

And one of the reasons we are more popular than we were four years ago -- we were very popular, but more popular -- is because they're so bad. They're so incompetent. They're so evil. They're so corrupt. And it makes us look that much better.

(END VIDEO CLIP)

BARTIROMO: And that is former President Trump on the campaign trail in Michigan and Wisconsin on Wednesday amid his ongoing trial in New York brought by Manhattan Democrat prosecutor Alvin Bragg.

On Thursday night, after spending the entire day in court, the 45th president made his way to a New York City firehouse in Midtown Manhattan to deliver boxes of pizza to the brave men and women of the FDNY, my heroes, Fire Department of New York.

A new poll from Emerson College and The Hill shows President Trump leading President Biden in seven swing states that account for a total of 93 electoral votes.

Joining me now with more on the presidential race is Co-Chair of the RNC Lara Trump.

Lara, good to see you. Thanks very much for being here.

And I want to start right there, because President Trump seems to be fitting in a bodega here and the Fire Department of New York there, trying to fit in campaign stops whenever he can. But the majority of his time is in a courtroom.

How are you raising money and putting President Trump in front of donors if he's got to be in New York all day long?

LARA TRUMP, CO-CHAIR, REPUBLICAN NATIONAL COMMITTEE: Yes.

Well, obviously, Maria, that's by design. They want to keep Donald Trump trapped in a courtroom and not able to go out and campaign. And their hope is that, somehow, that helps Joe Biden. But it's amazing to see.

It's almost like Sylvester the Cat and Tweety Bird. When Sylvester goes hard after Tweety Bird, it always backfires. And that's exactly what's happening to the Democrats right now, because you see, as you pointed out, Donald Trump's poll numbers continuing to go up.

And at the RNC and Trump campaign, we announced that our April fund-raising exceeded our expectations. We raised \$76 million. And the beauty of that is, the average donation, Maria, is under \$30. That means the people of this country understand what's at stake. They understand what is happening to this man, this lawfare that is being waged against him in an attempt to interfere in an election.

And they are fighting back. Even in the midst of this abysmal economy that Joe Biden has handed us, people are donating their money, DonaldJTrump.com, if anybody wants to support us, because they understand what is at stake right now.

So you're right. We get the weekends and we get Wednesdays, typically, with Donald Trump, the candidate, to go out and campaign. But he does these incredible stops. He goes, as you just pointed out, to the bodega in Harlem and gets a crowd Joe Biden couldn't even dream of. He goes and interacts with the FDNY, with construction workers at 6:30 in the morning.

It is earned media that Joe Biden will never get. He cannot do these kind of stops because no one will show up for him. The energy behind Donald Trump is palpable across this country. We just had a poll yesterday come out showing that the state of Washington, right now, Donald Trump is leading by one point, so it's within the margin of error, but nonetheless leading Joe Biden.

That tells you where this country is. We need Donald Trump back in the White House. And the lawfare and the communist tactics the Democrats are employing are backfiring.

BARTIROMO: Look, I think people want to see one-on-one Trump, Biden on stage for a debate with enough time to put their vote in.

But I believe the first debate happens after the early voting begins.

L. TRUMP: Yes, it's insane.

And we have called for more debates. Donald Trump has said any time, anywhere, any place he will debate Joe Biden. And, by the way, up until we got an interview between, of all people, Howard Stern and Joe Biden, we didn't even know if Joe Biden would commit to debates.

We couldn't get an answer from his campaign. It is imperative to see these two men on a stage, to see these two candidates who want to not just lead our country, but be the leader of the free world, head to head, face-to-face on a

debate stage. We need to hear from them, not only about what they accomplished in their presidencies, because we can compare two presidencies at this point, but their vision for the future of this country.

The truth is, we all know Joe Biden can't do it. His campaign has been very reluctant to even comment on this. But, as you point out, the Presidential Debate Commission has the first debate starting weeks after early voting, Maria.

We know that millions of people will cast a ballot for one of these two candidates before they get to see these two men debate. We need earlier debates. And we have said from the Trump campaign and the RNC, if they are not willing to move those debates forward, we would say to any network out there who would like to host a debate, Donald Trump will be there.

Joe Biden, we ask you to show up, because it is that important to the future of this country.

BARTIROMO: You have been saying for a while now that your priority is to ensure a transparent election.

And I see that -- the RNC and the Trump campaign filing a lawsuit in a battleground state to stop counting ballots past Election Day. What are you doing with regards to suing Nevada right now?

L. TRUMP: Yes, well, that's exactly right. You cannot have ballots counted, Maria, after elections are over.

And, right now, that is one of the many lawsuits we have out across this country to ensure that just that happens, that we have a free, fair and transparent election. So, in Nevada, as you pointed out, we are saying we want, on Election Day, that to be the last day that mail-in ballots can be counted.

And we have been very successful in a lot of lawsuits. A couple of weeks ago, we won a big lawsuit in the state of Pennsylvania. They wanted to take off dates from mail-in ballots, of course, the Democrats in an effort to make it easier to cheat.

BARTIROMO: Yes.

L. TRUMP: We pushed back on that. We won. And that set precedent for the entire country.

So whether it's Nevada, whether it's Pennsylvania, or whether it's in New York City, where we actually just had a big win, they were trying to encourage 800,000 noncitizens to vote. We had a bipartisan effort led by the RNC. We won there. They are not going to be able to do that.

And we are doing those things all across the country, because we can't be reactive. We have to be proactive. We have to look at this well ahead of Election Day and the election season that we now have in this country. We're doing everything from the RNC to ensure that that happens.

BARTIROMO: So what else can you tell us specifically that you're doing right now to ensure a transparent and free election in November, what, 5.5 months away now?

L. TRUMP: Yes. It's closing in fast.

And we have everything working at the RNC and the Trump campaign, protectthevote.com. I can't overstate how important it is for us to get people on our election integrity team. It is the largest division we have right now at the RNC.

If you want to volunteer out there to be a poll watcher, a poll worker, someone who can actually work in these polling locations and tabulation centers, we are now able to train you. We want you to join our team. If you're an attorney, we want attorneys volunteering as well because we want them in every single major polling location across this country to ensure that we are not waiting for weeks after Election Day.

We are going to strike at a moment's notice during early voting, during Election Day voting. We have to have our eyes on everything. So we want people to come volunteer. Michael Whatley, the chairman of the RNC, and I have announced that we want 100,000 people on our election integrity team by November 5. And we plan to meet that goal.

So I want to encourage everyone out there, please come join us, because, Maria, it is the most important thing.

BARTIROMO: All right, Lara, we will be watching all of that. Thanks very much for being here this morning.

L. TRUMP: Thank you so much.

BARTIROMO: All right, Lara Trump joining us.

Quick break and then: America in decline, yet Democrat judges and prosecutors are focused on taking down one man, and one man only, Donald Trump. A deep dive into Trump's New York trial and the classified documents case, as new details emerge on then-Vice President Joe Biden and the sensitive documents he walked away with.

Former prosecutor, Congressman and Director of National Intelligence John Ratcliffe on the state of affairs and the impact on national security.

Stay with us.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

REP. MICHAEL WALTZ (R-FL): I was shocked at how highly classified these documents are.

The media wants you to believe, oh, this was just some old Cold War stuff that old senile Biden maybe had in his garage from decades ago. No, it was recent. It was relevant. And, I mean, they had so many code words across it. I have had a clearance for 30 years. I had to ask what they meant.

(END VIDEO CLIP)

BARTIROMO: And that was Florida Congressman and House Intelligence Committee member Michael Waltz breaking news on this program last weekend with details on just how sensitive those classified documents are that were kept in President Biden's garage next to his Corvette, as well as at the Penn Biden Center.

The top secret documents dated back to Biden's tenure as both a vice president and a senator, which he had no authority to personally keep. Despite the national security risk, special counsel Robert Hur declined to charge Biden, in part because he said he's -- quote -- "an elderly man with a poor memory."

Meanwhile, special counsel Jack Smith is still pursuing his classified documents case against former President Trump. In a filing on Thursday, Trump's attorney has called for the 40-count indictment to be tossed, citing Hur's decision not to charge Biden.

And former Vice President Mike Pence admitted that he kept classified documents at his Indiana home after he left the White House. The DOJ declined to charge Pence, closing the case last year.

Then, this bombshell, the FBI admitting to misrepresenting the documents that they claimed to have taken from Trump estate Mar-a-Lago.

Joining me now with more in this "Sunday Morning Futures" exclusive on all of this is the former Director of National Intelligence and former prosecutor himself John Ratcliffe.

John, it's good to see you this morning. Thanks very much for being here.

JOHN RATCLIFFE, FORMER U.S. DIRECTOR OF NATIONAL INTELLIGENCE: Good morning, Maria.

BARTIROMO: I'm going to get to the classified documents issue in a moment and this misrepresentation by the FBI.

But, first, give us your legal aspect, legal perspective of the Manhattan DA's trial right now for Donald Trump.

RATCLIFFE: Well, it's been a train wreck for the prosecution.

Look, every witness that they have called so far has been a witness intending to harm Donald Trump. And, in fact, in every instance, they have at least in part helped Donald Trump with this case. And every witness that the state has called so far has also said that the state's most important witness, Michael Cohen, can't be believed, that he is essentially a pathological liar.

So, if this were a fair judge and a fair jury, the case already would have been dismissed or the case would be decided in the jurors' minds. But we don't have that, because we have a judge in this case who is allowing through his rulings the prosecutors to pursue an impossibility.

The case that they are prosecuting, Maria, is to try and show the jury that Donald Trump somehow magically, mystically, impossibly -- business records, entries in 2017 somehow influenced the presidential election of 2016. Their

whole case is premised on the idea that all of the conduct that they discuss, which is lawful, is somehow unlawful, and the judge is allowing them to do that.

And, of course, we know that is, in the end, is reversible error. But, in this case, we have a judge who voted for Joe Biden, donated to Joe Biden, whose daughter works for Joe Biden's vice president, Kamala Harris, and for Adam Schiff, and for the Democratic Party. And that has clearly been reflected in his rulings against President Trump throughout this trial.

And that's the only danger that President Trump has in this matter, because, from a legal standpoint, again, they're attempting to approve something that is absolutely legally impossible, and his conduct is absolutely lawful in every respect. And it is reversible error on any number of grounds when this case ultimately goes up, if it had to, with a verdict against the former president.

BARTIROMO: Now, you believe this is all coordinated, because you point out that there were some of these DAs that were meeting with White House counsel.

RATCLIFFE: Well, it absolutely is.

It was systematically coordinated. Look, this lawfare campaign, Maria, is the most unlawful and unconstitutional political persecution and instance of election interference that hopefully any of us will see in our lifetime.

I mean, as you know, what you have is the leading Republican presidential candidate and nominee in waiting. And the year before that election, there's not one, not two, not three, but four criminal indictments, all brought by Democratic prosecutors in either blue states or blue counties or by his opponent's own Department of Justice.

So it's absolutely out of bounds. It's absolutely coordinated. But it's also -- Maria, it's also failing. I mean, let's take inventory of where they are. In Georgia, the Fani Willis prosecution has all but collapsed under the weight of her own corruption.

In the Jack Smith matter, you have two cases. In the January 6 case, he's already been shot down by the Supreme Court once and is likely to be shot down shortly on the immunity issue.

And in the classified documents case that you referenced before, it's hanging by a thread, Maria, because, as you pointed out, he's now had to admit under oath that -- in filings with the court that they tampered with evidence and misrepresented or lied to the court about that, which then leaves us with this New York case, which really, at the end of the day, the only question for the jury in this case should be, who's more corrupt, the prosecutors or the judge?

BARTIROMO: So, in terms of the classified documents case, I remember the infamous picture that the FBI took of all those classified documents that they said that they took from Mar-a-Lago.

Specifically, tell me about what you're saying that, what evidence was tampered with, and did the FBI tamper with this?

RATCLIFFE: Yes, so that famous photograph, what we have now learned and the government has had -- Jack Smith and his prosecutors have had to admit, is that that was staged, and those top secret classified sheets that all the public saw and said, oh, my God, look at those top secret documents, those were placed there by the FBI.

And what Jack Smith admitted in court this week was that, in his words, they mishandled the classified documents and misrepresented those to the court. Maria, that's a kind way of saying, we tampered with the evidence and then we lied to the court about it.

And they got caught when President Trump's lawyers and the other co- defendants raised this issue and said, look, the documents here don't match up. The documents that were presented to us don't match the digitally scanned records of when they were taken from Mar-a-Lago.

And Jack Smith, not only did they tamper with that and lie to the court about it, but he's now admitted to the court that he doesn't know how that happened. He's only offered a number of possible explanations for how that could have happened.

So he's absolutely blown the chain of custody. And, again, he has a prosecutor, lead prosecutor in this case, Jay Bratt, who met with White House counsel and representative of the National Archives in -- several times in the weeks before Jack Smith was even appointed.

BARTIROMO: Wow.

APP-607

RATCLIFFE: Maria, this reeks -- this reeks of Crossfire Hurricane, when the Biden -- when the Obama-Biden administration fabricated evidence before the FISA court, lied to the court about it to pursue Donald Trump.

And now we're seeing it again in this classified documents case. The judge could dismiss this case at any point in time, Maria. I think the only reason that she has it is, she wants to document this publicly so that the public can see just how this case is being prosecuted, how unfairly Donald Trump has been persecuted in this matter by Joe Biden's Department of Justice.

BARTIROMO: Let me move on, John, and ask you about the issues of the day with regard to foreign policy.

There is a, what, ultimatum on the table for Hamas. They either have to agree to give up and give these -- let these hostages free or Netanyahu is promising to go into Rafah and take down the Hamas terrorists. Tell me how you see that unfolding.

And I want to get your take on the China role here, because we are waiting to see some kind of a tough stance against communist China for all of this bad behavior, but it just hasn't happened from this administration.

RATCLIFFE: Well, and it's not going to happen. It hasn't happened, and it's not going to happen.

But with respect to what's happening in Israel is, yes, Prime Minister Netanyahu has given an ultimatum to Hamas: You have one week to accept a six-week cease-fire in exchange for releasing the hostages.

Hamas is responding so far and said, no, you have to promise to end the war.

You know who's agreeing with Hamas? The Biden administration. We should be helping Benjamin Netanyahu. We should do everything we can to allow him to go into Rafah and eradicate the remaining four battalions of Hamas that are in -- still in Gaza.

BARTIROMO: Yes.

RATCLIFFE: Because, Maria, what happens with Hamas here is a blueprint for what's going to happen with Hezbollah, the Houthis, with Al Qaeda, with ISIS, with every radical Islamic group.

BARTIROMO: Yes.

RATCLIFFE: And we should be supporting Israel in this struggle, not supporting Hamas, which is what the Biden administration is doing and what China is doing.

So, at the same day that Antony Blinken left Beijing last week, the People's Republic of China received a delegation from, yes, you guessed it, Hamas. So they are working in that region to help Hamas, and they are working in the United States through TikTok and through their assets here in the United States to foment unrest in this country.

BARTIROMO: Yes.

John, one thing I want to know real quick -- we have got to jump -- but all of these Chinese nationals that have come through the border, the open border, 24,000, 25,000 just since October, on top of another 25,000 the year before, do we have any knowledge in terms of whether or not any of them were saboteurs in these -- college campus unrest?

I mean, we're trying to understand who's behind all of this and also trying to understand why so many Chinese nationals have come through the wide-open border on Joe Biden's watch.

RATCLIFFE: Yes, well, we wouldn't know because Joe Biden did nothing to track these Chinese nationals coming into the country.

BARTIROMO: Right.

RATCLIFFE: But you would be insane not to think that, of the 24,000 that have just recently come in, that they're not playing some role in what China's trying to do, which is to create chaos in this country.

We know that they're doing it through TikTok. So, many of the assets that they have now brought into this country that we know from our intelligence that they have are likely contributing on the ground to foment this chaos across the country on our campuses.

BARTIROMO: OK. Well, it's a story that I will certainly follow.

Settings

← Post

Senator John Fetterman

@SenFettermanPA

Every single American company must bend to the Chinese communist government's will to operate in China.

I voted yes to force this sale to make TikTok safer for our children and national security.

Their arrogance is astounding.

The New York Times

BREAKING

TikTok Sues U.S. Government Over Law Forcing Sale or Ban

The social media company and its Chinese parent, ByteDance, sued to challenge the new law, saying it violated users' First Amendment rights.

1:06 PM · May 7, 2024 · 303K Views

441 Reposts

154 Quotes

3,340 Likes

46 Bookmarks

🗨

↻

❤

🔖 46

⬆

New to X?

Sign up now to get your own personalized timeline!

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Relevant people

Senator John Fetterman

@SenFettermanPA

United States Senator fighting for the people of the Commonwealth of Pennsylvania.

Follow

Something went wrong. Try reloading.

↻ Retry

[Terms of Service](#) [Privacy Policy](#) [Cookie Policy](#) [Accessibility](#) [Ads info](#) [More ...](#) © 2024 X Corp.

Don't miss what's happening
People on X are the first to know.

Log in

Sign up

APP-609

https://x.com/SenFettermanPA/status/1787891840022139280

1/1

Exhibit Q

TikTok Deal Is Complicated by New Rules From China Over Tech Exports

 [nytimes.com/2020/08/29/technology/china-tiktok-export-controls.html](https://www.nytimes.com/2020/08/29/technology/china-tiktok-export-controls.html)

Paul Mozur, Raymond Zhong, David McCabe

August 29, 2020

SKIP ADVERTISEMENT

As the sale of TikTok enters its final stages, Beijing is saying it wants the last word.

In a bureaucratic two-step, China on Friday updated its export control rules to cover a variety of technologies it deemed sensitive, including technology that sounded much like TikTok's personalized recommendation engine. Then on Saturday, the country's official Xinhua news agency published commentary by a professor who said the new rule would mean that the video app's parent, the Chinese internet giant ByteDance, might need a license to sell its technology to an American suitor.

Beijing's last-minute assertion of authority is an unexpected wrinkle for a deal as two groups race to buy TikTok's U.S. operations before the Trump administration bans the app. Taken together, the rule change and the commentary in official media signaled China's intention to dictate terms over a potential deal, though experts said it remained unclear whether the Chinese government would go as far as to sink it.

The moves from Beijing ensnare TikTok and potential American buyers including Microsoft and Oracle, wedging them in the middle of a tussle between the United States and China over the future of global technology. Beijing's displeasure alone could scare off TikTok's suitors, many of whom have operations in China. TikTok is the most globally successful app ever produced by a Chinese company, and the conflict over its fate could further fracture the internet and plunge the world's two largest economies into a deeper standoff.

"At a minimum they're flexing their muscles and saying, 'We get a say in this and we're not going to be bystanders,'" said Scott Kennedy, a senior adviser at the Washington-based Center for Strategic and International Studies who studies Chinese economic policy.

SKIP ADVERTISEMENT

"It could be an effort to outright block the sale, or just raise the price, or attach conditions to it to give China leverage down the road," he said. He added that it showed a rare bit of consensus between China and the United States that both agreed ByteDance was a national security priority.

If Beijing blocks the sale of TikTok, it would effectively be calling the Trump administration's bluff, forcing the U.S. government to actually go through with restricting the app and potentially incurring the wrath of its legions of influencers and fans. Ordering companies like

Apple and Google to take down TikTok in app stores globally could also prompt further anger against the Trump administration and even lawsuits.

ByteDance and Oracle declined to comment on the rule changes and the Xinhua article. Microsoft did not have immediate comment. The U.S. Department of Commerce did not respond to requests for comment. The White House did not immediately respond to a request for comment. But Beijing's move could risk empowering the more hawkish members of Mr. Trump's team and igniting an even more forceful response from the administration, which has said that it could take more measures to block tech companies like Alibaba and Baidu from doing business in the United States.

China's changes to its export rules came just as ByteDance had signaled that it was close to reaching a resolution on the future of TikTok's business in the United States. President Trump this month issued an executive order restricting Americans' dealings with TikTok beginning in mid-September. He and other White House officials have said the app could be a Trojan Horse for data gathering by the Chinese Communist Party, an accusation that ByteDance has denied. That set off the deal negotiations.

Chinese officials have denounced the Trump administration's treatment of TikTok, characterizing it as "bullying."

SKIP ADVERTISEMENT

In Friday's update to the export control rules, China's Commerce Ministry and its Science and Technology Ministry restricted the export of "technology based on data analysis for personalized information recommendation services." TikTok plays up its ability to use technology to understand users' interests and fill their feeds with more of what they will enjoy watching.

In the Saturday article published by Xinhua, a professor of international trade at China's University of International Business and Economics, Cui Fan, said that ByteDance's technologies would most likely be covered by the new export controls.

"If ByteDance plans to export relevant technologies, it should go through the licensing procedures," the article cited Mr. Cui as saying. Any sale of TikTok would most likely require the transfer overseas of code and technical services, the article said.

"It is recommended that ByteDance seriously study the adjusted catalog, and carefully consider whether it is necessary to suspend the substantive negotiation of related transactions, perform the legal declaration procedures and then take further actions as appropriate," Mr. Cui was quoted as saying.

Mr. Kennedy said that it was exceedingly rare for a professor to make comments about a specific, in-progress deal, and that it signaled that ByteDance would now have to consult the Chinese authorities about the controls.

SKIP ADVERTISEMENT

China has previously used bureaucratic procedure to block commercial deals without appearing to do so outright. In 2018, Qualcomm called off a \$44 billion deal to buy the Dutch chip maker NXP Semiconductors after Chinese regulators simply failed to either approve or reject the transaction. Beijing's prolonged antitrust review was seen as a form of leverage over trade talks with the Trump administration, though China's Ministry of Commerce denied that the two matters were related.

In other industries, too, foreign companies including Microsoft, Volkswagen and Chrysler have been investigated for what China says are anticompetitive practices. Beijing has rejected the charge, made by American business groups, that it uses laws like antimonopoly rules to advance industrial policy.

The use of export controls was novel, but it mirrors similar regulatory hurdles thrown at Chinese companies by the Trump administration. The White House order that prompted TikTok's sale cited national security concerns, and the United States has repeatedly blocked Chinese bids for companies with sensitive technologies as well as data.

Mr. Kennedy said China's ultimate motivation in holding up or thwarting the deal could be, at minimum, a "kneejerk assertion of sovereignty."

Doug Jacobson, a partner at the Washington trade law firm Jacobson Burton Kelley, said the impact of China's new rules would hinge on how essential the technology in question was to TikTok's app and whether that technology was part of a sale.

SKIP ADVERTISEMENT

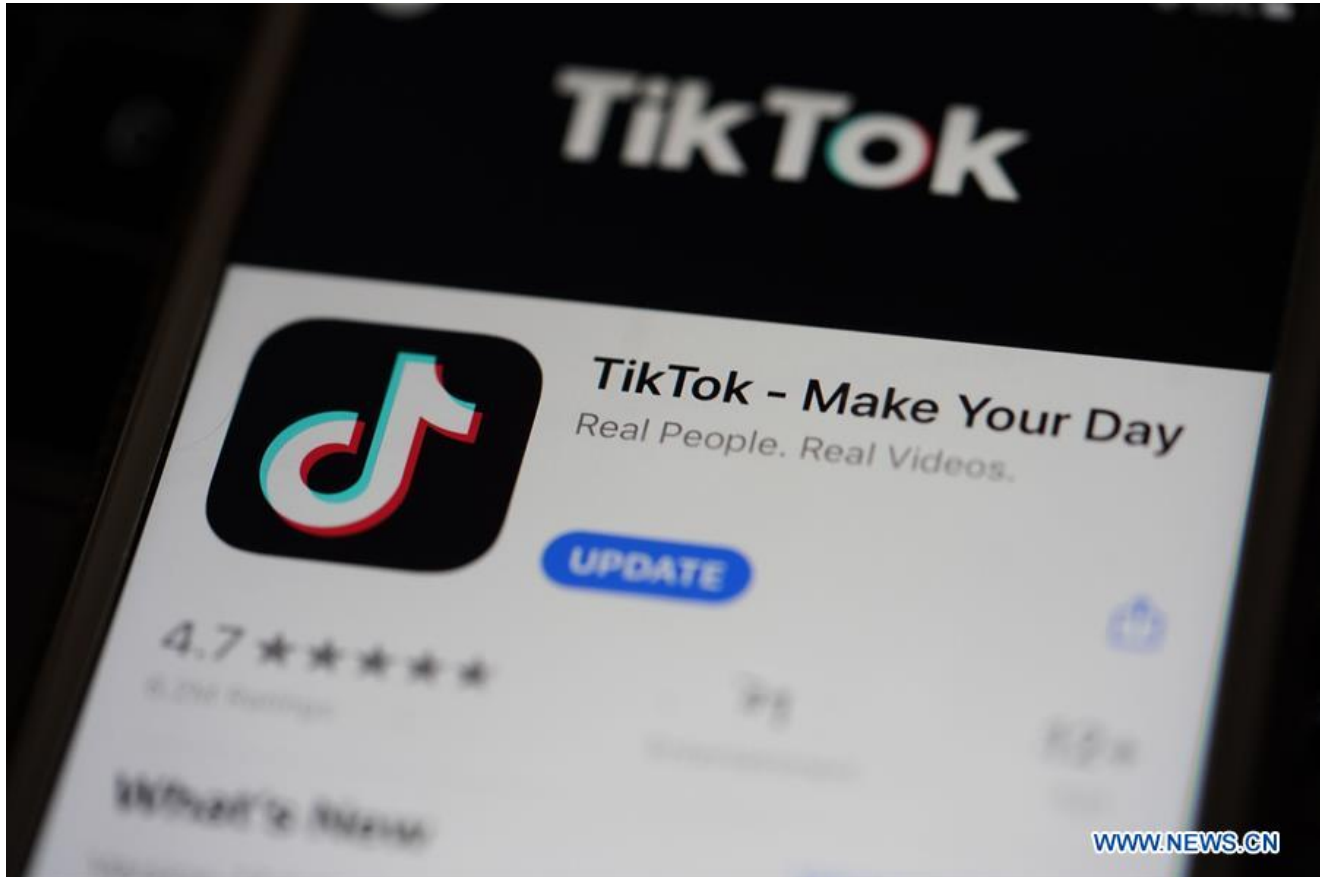
"It's going to depend on how the transaction is structured and also just how this technology is embedded or incorporated into the code itself," he said.

Exhibit R

Planned TikTok deal entails China's approval under revised catalogue: expert

 xinhuanet.com/english/2020-08/30/c_139329598.htm

Source: Xinhua| 2020-08-30 22:45:42|Editor: huaxia



The logo of TikTok is seen on a smartphone screen in Arlington, Virginia, the United States, Aug. 30, 2020. (Xinhua/Liu Jie)

BEIJING, Aug. 30 (Xinhua) -- ByteDance, the parent company of TikTok, will need to comply with approval procedures under China's latest revision to the catalogue of technologies that are subject to export bans or restrictions, regarding the planned selling of the video-sharing app's U.S. operations, an expert observed.

As a fast-growing innovative enterprise, ByteDance has many cutting-edge technologies in artificial intelligence and other fields, and some technologies may have been covered by the adjusted catalogue, Professor Cui Fan at the University of International Business and Economics told Xinhua in an interview commenting on the catalogue.

The revised catalogue, released jointly on Friday by the Ministry of Commerce and the Ministry of Science and Technology, added a total of 23 items subject to export restrictions.

Two new items under the category of information processing technology in the computer service industry were cited by Cui as relevant in the TikTok deal, which was the "personalized information push service technology based on data analysis" and "artificial intelligence interactive interface technology."

The rapid development of ByteDance's international businesses has been built on the strong technical support based in China, Cui said, noting that the company's act of offering core algorithm services to overseas branches constitutes a typical export of technical services.

"For the international business to continue to operate smoothly, no matter who its new owner and operator are, it is highly likely that there will need to be a transfer of software codes or right of use from inside China to outside China," Cui said. "Technical services provision from inside China to outside China may also be needed."

"Therefore, it is suggested that ByteDance carefully study the revised catalogue, seriously and carefully consider whether it is necessary to suspend substantive negotiations on relevant transactions, comply with statutory application and reporting procedures, and then take further actions as appropriate," Cui said. Enditem

Exhibit S

CHARLES E. SCHUMER

Majority Leader

NEW YORK

United States Senate

WASHINGTON, DC 20510-3203

April 5, 2024

Dear Colleague:

I want to thank you all again for your work last month to pass a strong bipartisan funding package that rejected MAGA extremism, put the needs of the country first, and averted a harmful and pointless government shutdown. The Appropriations package will go a long way to supporting American families, strengthening our economy, and safeguarding our national security. We also avoided most of the draconian cuts and poison pills that the hard-right pushed for months. This was no small feat and is a tremendous credit to leadership on both sides, particularly our Appropriations Chair Murray and Vice Chair Collins.

When we return, we have busy agenda facing us. First, we will continue our work to confirm President Biden's well qualified and diverse nominees. Speaker Johnson has indicated that the House Impeachment Managers plan to deliver the articles of impeachment on Wednesday. The Senate will receive the managers as they present the articles of impeachment for Secretary Mayorkas to the Senate. Please be advised that all Senators will be sworn in as jurors in the trial the day after the articles are presented, and Senate President Pro Tempore Patty Murray will preside. I remind Senators that your presence next week is essential.

Additionally, we face an April 19 deadline on reauthorizing FISA. The House is working on a path forward for their legislation. The Senate must be ready to act quickly on a bipartisan basis to ensure these vital national security authorities do not lapse.

Off the floor, we will continue to keep pressure on the House to act on the Senate-passed national security supplemental that would provide desperately needed funding to Ukraine in their fight against Putin. The Senate bill has sat on Speaker Johnson's desk for more than 50 days. The longer that the national security supplemental sits on Speaker Johnson's desk, the more desperate the situation in Ukraine becomes.

I have spoken with Speaker Johnson, and I believe that he understands the threat of further delaying the national security supplemental. However, Speaker Johnson has to ultimately decide for himself whether or not he will do the right thing for Ukraine, for America and for democracy around the world or if he'll allow the extreme MAGA wing of his party to hand Vladimir Putin a victory. It is a matter of the highest urgency that Speaker Johnson and House Leadership put the Senate's bipartisan supplemental package on the House floor, because I am confident that if he puts it on the floor, it will pass.

Like so many of you, I was shocked and saddened by the tragic collapse of Francis Scott Key Bridge. I've spoken with Maryland Senators Senator Ben Cardin and Senator Van Hollen and offered any help needed as Baltimore works to recover. This morning the Biden administration submitted an authorizing request for the Francis Scott Key Bridge and Port of Baltimore. It will take bipartisan cooperation for the Senate to act quickly to help reopen the Port of Baltimore, a major artery for commerce, and rebuild the Key Bridge as quickly as possible.

APP-618

In addition to continuing to confirm President Biden's nominees, there are a range of policy areas where we could advance legislation to help the American people, if we can get bipartisan cooperation from our Republican colleagues. The authorization for FAA expires on May 10 and bicameral and bipartisan work is underway on that important piece of legislation. Commerce Committee Chairwoman Cantwell and her team are working tirelessly to finalize an agreement and pass the FAA reauthorization in May.

In the weeks and months ahead, we have the opportunity to make progress on bipartisan bills that enhance our national security, advance online safety for kids and promote innovation, expand the Child Tax Credit, work on a path forward on Tik Tok legislation, combat the fentanyl crisis, hold failed bank executives accountable, address rail safety, ensure internet affordability, safeguard cannabis banking, outcompete the Chinese government, lower the cost of prescription drugs like insulin while expanding access to health care, and more. There are many important, bipartisan issues this Congress could address this year, and I hope our Senate Republican colleagues don't allow the ultra-right wing of their party to derail progress on these bipartisan bills.

Unfortunately, just last month we saw just how committed House Republicans are to the extreme the MAGA Republican agenda when the Republican Study Committee released their dangerous and disastrous budget plan. They're doubling down on the hard-right's war on women by endorsing a national ban on abortion with zero exceptions for rape or incest and endangering access to IVF. They continue their relentless attacks on social security and called for raising the retirement age. Their plan advocates for repealing \$35 insulin for seniors on Medicare and taking away Medicare's authority to negotiate cheaper drug prices. And, of course, they propose providing trillions of dollars in tax breaks for the ultra-wealthy and trillions of dollars in budget cuts to the Children's Health Insurance Program and the ACA.

These are many of the same policies Democrats fought to keep out of the appropriations bills this year, and as long as Senate Democrats are in the majority we will ensure that this extreme MAGA agenda does not become law.

I have said repeatedly this Congress, with divided government, bipartisanship and compromise are the only ways to make progress and get things done that will help the American people. Democrats have an ambitious agenda to help the American people, and if our Senate Republican colleagues are sincere about passing bipartisan legislation and willing to reject the extreme MAGA demands, we are ready to work with them to find compromise and get as much done as we can.

I look forward to working with you all in the coming weeks to continue delivering results for the American people.

Sincerely,



Charles E. Schumer
United States Senator

Exhibit T

Mike Johnson's Letter Sparks New Flood of Republican Backlash

N [newsweek.com/mike-johnsons-letter-sparks-new-flood-republican-backlash-1891376](https://www.newsweek.com/mike-johnsons-letter-sparks-new-flood-republican-backlash-1891376)

Rachel Dobkin

April 17, 2024

By Rachel Dobkin
Weekend Reporter

House Speaker Mike Johnson's letter about foreign funding bills sparked a new flood of Republican backlash on social media on Wednesday.

It has been months since the Senate passed a \$95-billion funding package which would give aid to Ukraine in its fight against Russia, money to Israel in its war with Hamas, and funds for Taiwan to combat Chinese aggression.

However, the House has yet to act on the bill and instead, Johnson, a Louisiana Republican, told colleagues in a letter on Wednesday that the language of three separate funding bills will be posted today.

"After significant member feedback and discussion, the House Rules Committee will be posting soon today the text of three bills that will fund America's national security interests and allies in Israel, the Indo-Pacific, and Ukraine, including a loan structure for aid, and enhanced strategy and accountability," Johnson wrote in the letter that has circulated on social media.

"These will be brought to the floor under a structured rule that will allow for an amendment process, alongside a fourth bill that includes the REPO Act, TikTok bill, sanctions and other measures to confront Russia, China, and Iran."



House Speaker Mike Johnson on April 16, 2024, in Washington D.C. Johnson's letter about foreign funding bills sparked a new flood of Republican backlash on social media on Wednesday. Win McNamee/Getty Images

Begin your day with a curated outlook of top news around the world and why it matters.

By clicking on SIGN ME UP, you agree to Newsweek's Terms of Use & Privacy Policy. You may unsubscribe at any time.

The REPO Act refers to the Rebuilding Economic Prosperity and Opportunity for Ukrainians Act. It allows the president of the United States to confiscate sovereign assets of the Russian Federation that are directly or indirectly owned by the government, states the Lawfare website.

The House speaker said that the committee will also post text for a bill on border security that "includes the core components of H.R.2," which is a piece of tough immigration legislation that passed on the House last May, but was blocked by the Democratic-led Senate.

"By posting text of these bills as soon as they are completed, we will ensure time for a robust amendment process. We expect the vote on final passage on these bills to be on Saturday evening," Johnson added in the letter.

Tensions between Johnson and members of his own party in the House have already been high with Rep. Marjorie Taylor Greene of Georgia introducing a motion to vacate him from the speaker seat last month and Rep. Thomas Massie, from Kentucky, writing on social media on Tuesday that he told Johnson that he is co-sponsoring Greene's motion.

Johnson said he is not resigning and called any attempt to oust him as Speaker "absurd." *Newsweek* has reached out to Johnson's office via email for comment.

Johnson's new letter seemed to cause more backlash on how he is handling foreign funding and the U.S.-Mexico border, which is at the heart of Greene's motion to vacate.

Reacting to the letter on Wednesday, Greene wrote on X, formerly Twitter, "News flash for Speaker Johnson, we have already passed HR2, the Senate has it and refuses to secure our border, they want 5,000 illegals per day to come in.

"The House passed \$14 Billion for Israel aid in Nova and the Senate refuses to pass it. You, Speaker Johnson, voted against \$300 million for Ukraine before we gave you the gavel along with the majority of Republicans, no one understands why it is now your top priority to give Ukraine \$60 billion more dollars."

News flash for Speaker Johnson, we have already passed HR2, the Senate has it and refuses to secure our border, they want 5,000 illegals per day to come in.

The House passed \$14 Billion for Israel aid in Nova and the Senate refuses to pass it.

You, Speaker Johnson, voted...

— Rep. Marjorie Taylor Greeneus (@RepMTG) April 17, 2024

Greene was referencing a border deal that previously failed in the Senate, which would have enabled U.S. Department of Homeland Security officials to detain and deport migrants if there is an average of 5,000 or more migrant encounters a day over seven consecutive days or if there are 8,500 or more encounters in a single day.

"You are seriously out of step with Republicans by continuing to pass bills dependent on Democrats. Everyone sees through this."

Sen. J.D. Vance, an Ohio Republican, wrote, "Rumored course of action in the House: Combine Ukraine and Israel aid, with other Biden boondoggles. Send it all to the Senate as a combined package. Then let the House vote on a fake border security package that has no chance. Betrayal. And stupid politics to boot."

"The Republican Speaker of the House is seeking a rule to pass almost \$100 billion in foreign aid—while unquestionably, dangerous criminals, terrorists, & fentanyl pour across our border. The border 'vote' in this package is a watered-down dangerous cover vote. I will oppose," Rep. Chip Roy, a Texas Republican said.

"Anything less than tying Ukraine aid to real border security fails to live up to @SpeakerJohnson's own words just several weeks ago. Our constituents demand—and deserve—more from us," Rep. Scott Perry, representing a Pennsylvania district, wrote.

Former Republican congressman from Illinois Adam Kinzinger, who has been critical of the far-right faction in his party, slammed Johnson for not doing enough on *CNN Newsroom with Jim Acosta* on Wednesday.

"The fact that we are six months, frankly, after we should have passed aid to Ukraine, and three months after the Senate did, and it has been sitting in the House. Don't call yourself a 'wartime speaker' if you're unwilling to do what's needed to be done in a wartime," Kinzinger said.

Kinzinger's comments come after Johnson called himself a "wartime speaker" during a press conference on Tuesday.

Newsweek is committed to journalism that's factual and fair.

Hold us accountable and submit your rating of this article on the meter.

[Request Reprint & Licensing](#) [Submit Correction](#) [View Editorial Guidelines](#)

About the writer

Rachel Dobkin

Rachel Dobkin is a Newsweek reporter based in New York. Her focus is reporting on politics.

Rachel joined Newsweek in ... [Read more](#)

To read how Newsweek uses AI as a newsroom tool, [Click here](#).

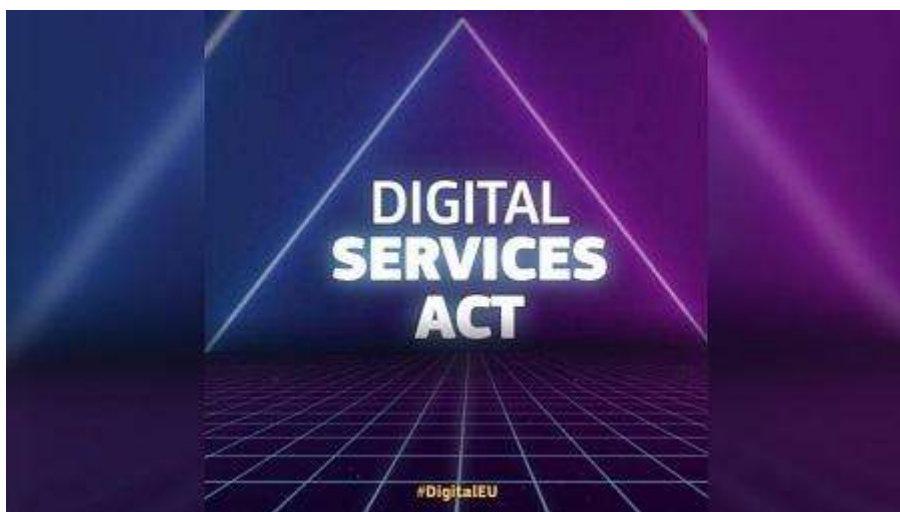
Exhibit U



Shaping Europe's digital future

DSA: Very large online platforms and search engines

Very large online platforms and search engines are those with over 45 million users in the EU. They must comply with the most stringent rules of the DSA.



The DSA classifies platforms or search engines that have more than 45 million users per month in the EU as very large online platforms (VLOPs) or very large online search engines (VLOSEs). The Commission has begun to designate VLOPs or VLOSEs based on user numbers provided by platforms and search engines, which regardless of size, they were [required to publish by 17 February 2023](#).

Platforms and search engines will need to update these figures at least every 6 months as explained on [DSA: Guidance on the requirement to publish user numbers](#).

Once the Commission designates a platform as a VLOP or a search engine as a VLOSE, the designated online service has 4 months to comply with the DSA. The designation triggers specific rules that tackle the particular risks such large services pose to Europeans and society when it comes to illegal content, and their impact on fundamental rights, public security, and wellbeing.

The Commission will revoke its decision if the platform or search engine does not reach the threshold of 45 million monthly users anymore during one full year.

Obligations for VLOPs and VLOSEs

Once the Commission has designated a platform or a search engine, it has four months to comp., with the DSA.

For example it needs to:

- establish a point of contact for authorities and users
- report criminal offenses
- have user-friendly terms and conditions
- be transparent as regards advertising, recommender systems or content moderation decisions

They also must follow the rules that focus only on VLOPs and VLOSEs due to their size and the potential impact they can have on society. This means that they must identify, analyse, and assess systemic risks that are linked to their services. They should look, in particular, to risks related to:

- illegal content
- fundamental rights, such as freedom of expression, media freedom and pluralism, discrimination, consumer protection and children's rights
- public security and electoral processes
- gender-based violence, public health, protection of minors, and mental and physical wellbeing

Once the risks are identified and reported to the Commission for oversight, VLOPs and VLOSEs are obliged to put measures in place that mitigate these risks. This could mean adapting the design or functioning of their services or changing their recommender systems. They could also consist of reinforcing the platform internally with more resources to better identify systemic risks.

Those designated as VLOPs or VLOSEs will also have to:

- establish an internal compliance function that ensures that the risks identified are mitigated
- be audited by an independent auditor at least once a year and adopt measures that respond to the auditor's recommendations
- share their data with the Commission and national authorities so that they can monitor and assess compliance with the DSA
- allow vetted researchers to access platform data when the research contributes to the detection, identification and understanding of systemic risks in the EU
- provide an option in their recommender systems that is not based on user profiling
- have a publicly available repository of advertisements

Quick links

List of the designated VLOPs and VLOSEs (<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-slops>)

DSA: Guidance on the requirement to publish user numbers (<https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers>)

DSA FAQ (<https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-functions-and-answers>)

Latest News

PRESS RELEASE | 11 June 2024

Commission services sign administrative arrangement with Australian eSafety Commissioner to support the enforcement of social media regulations

(</en/news/commission-services-sign-administrative-arrangement-australian-esafety-commissioner-support>)

Today, the Commission services responsible for the enforcement of the Digital Services Act (DSA) have signed an administrative arrangement with the eSafety

PRESS RELEASE | 11 June 2024

Commission services sign administrative arrangement with Australian eSafety Commissioner to support the enforcement of social media regulations

[\(/en/news/commission-services-sign-administrative-arrangement-australian-esafety-commissioner-support-0\)](#)

Today, the Commission services responsible for the enforcement of the Digital Services Act (DSA) have signed an administrative arrangement with the eSafety Commissioner – the independent regulator for online safety in Australia.

PRESS RELEASE | 07 June 2024

Statement by Commissioner Breton on steps announced by LinkedIn to comply with DSA provisions on targeted advertisement

[\(/en/news/statement-commissioner-breton-steps-announced-linkedin-comply-dsa-provisions-targeted-advertisement\)](#)

The Commission takes note of LinkedIn's announcement that it has fully disabled the functionality allowing advertisers to target LinkedIn users with ads on the basis of their membership in LinkedIn Groups in the EU Single Market.

NEWS ARTICLE | 06 June 2024

EU Internet Forum welcomes new members to combat harmful and illegal content online

[\(/en/news/eu-internet-forum-welcomes-new-members-combat-harmful-and-illegal-content-online\)](#)

On June 4, 2024, the EU Internet Forum (EUIF) has met to expand its membership. Amazon, SoundCloud, Mistral AI, DailyMotion, and the Institute for Strategic Dialogue - a civil society organization - have become members of the EU Internet Forum.

[Browse Digital Services Act Package](#) > [\(/en/related-content?topic=193\)](#)

Related Content

Big Picture

The Digital Services Act package (</en/policies/digital-services-act-package>).

The Digital Services Act and Digital Markets Act aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.

See Also

Trusted flaggers under the Digital Services Act (DSA) (</en/policies/trusted-flaggers-under-dsa>).

Under DSA, trusted flaggers are responsible for detecting potentially illegal content and alert online platforms. They are entities designated by the national Digital Services Coordinators.

European Board for Digital Services (</en/policies/dsa-board>).

The European Board for Digital Services is an independent advisory group that has been established by the Digital Services Act, with effect from 17 February 2024.

DSA whistleblower tool (</en/policies/dsa-whistleblower-tool>)

The DSA (Digital Services Act) whistleblower tool allows employees and other insiders to report harmful practices of Very Large Online Platforms and Search Engines (VLOPs/VLOSEs)

Digital Services Coordinators (</en/policies/dsa-dscs>)

Digital Services Coordinators help the Commission to monitor and enforce obligations in the Digital Services Act (DSA).

How the Digital Services Act enhances transparency online (</en/policies/dsa-brings-transparency>)

The Digital Services Act (DSA) details a range of actions to promote transparency and accountability of online services, without hindering innovation and competitiveness.

Supervision of the designated very large online platforms and search engines under DSA (</en/policies/list-designated-vlops-and-vloses>)

This page provides an overview of the designated Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) supervised by the Commission and the main enforcement activities.

The impact of the Digital Services Act on digital platforms (</en/policies/dsa-impact-platforms>)

Since August 2023, platforms have already started to change their systems and interfaces according to the Digital Services Act (DSA) to provide a safer online experience for all.

The enforcement framework under the Digital Services Act (</en/policies/dsa-enforcement>)

The enforcement of the Digital Services Act (DSA) includes a full set of investigative and sanctioning measures that can be taken by national authorities and the Commission.

The cooperation framework under the Digital Services Act (</en/policies/dsa-cooperation>)

The Digital Services Act (DSA) provides a framework for cooperation between the Commission, EU and national authorities to ensure platforms meet its obligations.

DSA: Making the online world safer (</en/policies/safer-online>)

Find out how the DSA can make the online world safer and protect your fundamental rights.

European Centre for Algorithmic Transparency (</en/policies/ecat>)

The European Centre for Algorithmic Transparency (ECAT) is committed to improved understanding and proper regulation of algorithmic systems.

Last update

21 February 2024

Print as PDF

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 19 October 2022

on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,Having regard to the opinion of the Committee of the Regions ⁽²⁾,Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

- (1) Information society services and especially intermediary services have become an important part of the Union's economy and the daily life of Union citizens. Twenty years after the adoption of the existing legal framework applicable to such services laid down in Directive 2000/31/EC of the European Parliament and of the Council ⁽⁴⁾, new and innovative business models and services, such as online social networks and online platforms allowing consumers to conclude distance contracts with traders, have allowed business users and consumers to impart and access information and engage in transactions in novel ways. A majority of Union citizens now uses those services on a daily basis. However, the digital transformation and increased use of those services has also resulted in new risks and challenges for individual recipients of the relevant service, companies and society as a whole.
- (2) Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation, imposing, in particular, diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks. Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty on the Functioning of the European Union (TFEU), comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured, taking into account the inherently cross-border nature of the internet, which is generally used to provide those services. The conditions for the provision of intermediary services

⁽¹⁾ OJ C 286, 16.7.2021, p. 70.⁽²⁾ OJ C 440, 29.10.2021, p. 67.⁽³⁾ Position of the European Parliament of 5 July 2022 (not yet published in the Official Journal) and decision of the Council of 4 October 2022.⁽⁴⁾ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

2. Providers of intermediary services shall mandate their legal representatives for the purpose of being addressed in addition to or instead of such providers, by the Member States' competent authorities, the Commission and the Board, on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation. Providers of intermediary services shall provide their legal representative with necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the Member States' competent authorities, the Commission and the Board, and to comply with such decisions.

3. It shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the provider of intermediary services.

4. Providers of intermediary services shall notify the name, postal address, email address and telephone number of their legal representative to the Digital Services Coordinator in the Member State where that legal representative resides or is established. They shall ensure that that information is publicly available, easily accessible, accurate and kept up to date.

5. The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Article 14

Terms and conditions

1. Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.

2. Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.

3. Where an intermediary service is primarily directed at minors or is predominantly used by them, the provider of that intermediary service shall explain the conditions for, and any restrictions on, the use of the service in a way that minors can understand.

4. Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.

5. Providers of very large online platforms and of very large online search engines shall provide recipients of services with a concise, easily-accessible and machine-readable summary of the terms and conditions, including the available remedies and redress mechanisms, in clear and unambiguous language.

6. Very large online platforms and very large online search engines within the meaning of Article 33 shall publish their terms and conditions in the official languages of all the Member States in which they offer their services.

Article 15

Transparency reporting obligations for providers of intermediary services

1. Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. Those reports shall include, in particular, information on the following, as applicable:

- (a) for providers of intermediary services, the number of orders received from Member States' authorities including orders issued in accordance with Articles 9 and 10, categorised by the type of illegal content concerned, the Member State issuing the order, and the median time needed to inform the authority issuing the order, or any other authority specified in the order, of its receipt, and to give effect to the order;
- (b) for providers of hosting services, the number of notices submitted in accordance with Article 16, categorised by the type of alleged illegal content concerned, the number of notices submitted by trusted flaggers, any action taken pursuant to the notices by differentiating whether the action was taken on the basis of the law or the terms and conditions of the provider, the number of notices processed by using automated means and the median time needed for taking the action;
- (c) for providers of intermediary services, meaningful and comprehensible information about the content moderation engaged in at the providers' own initiative, including the use of automated tools, the measures taken to provide training and assistance to persons in charge of content moderation, the number and type of measures taken that affect the availability, visibility and accessibility of information provided by the recipients of the service and the recipients' ability to provide information through the service, and other related restrictions of the service; the information reported shall be categorised by the type of illegal content or violation of the terms and conditions of the service provider, by the detection method and by the type of restriction applied;
- (d) for providers of intermediary services, the number of complaints received through the internal complaint-handling systems in accordance with the provider's terms and conditions and additionally, for providers of online platforms, in accordance with Article 20, the basis for those complaints, decisions taken in respect of those complaints, the median time needed for taking those decisions and the number of instances where those decisions were reversed;
- (e) any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied.

2. Paragraph 1 of this Article shall not apply to providers of intermediary services that qualify as micro or small enterprises as defined in Recommendation 2003/361/EC and which are not very large online platforms within the meaning of Article 33 of this Regulation.

3. The Commission may adopt implementing acts to lay down templates concerning the form, content and other details of reports pursuant to paragraph 1 of this Article, including harmonised reporting periods. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

SECTION 2

Additional provisions applicable to providers of hosting services, including online platforms

Article 16

Notice and action mechanisms

1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means.

6. The Commission shall notify its decisions pursuant to paragraphs 4 and 5, without undue delay, to the provider of the online platform or of the online search engine concerned, to the Board and to the Digital Services Coordinator of establishment.

The Commission shall ensure that the list of designated very large online platforms and very large online search engines is published in the *Official Journal of the European Union*, and shall keep that list up to date. The obligations set out in this Section shall apply, or cease to apply, to the very large online platforms and very large online search engines concerned from four months after the notification to the provider concerned referred to in the first subparagraph.

Article 34

Risk assessment

1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

They shall carry out the risk assessments by the date of application referred to in Article 33(6), second subparagraph, and at least once every year thereafter, and in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified pursuant to this Article. This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:

- (a) the dissemination of illegal content through their services;
- (b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;
- (c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;
- (d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

2. When conducting risk assessments, providers of very large online platforms and of very large online search engines shall take into account, in particular, whether and how the following factors influence any of the systemic risks referred to in paragraph 1:

- (a) the design of their recommender systems and any other relevant algorithmic system;
- (b) their content moderation systems;
- (c) the applicable terms and conditions and their enforcement;
- (d) systems for selecting and presenting advertisements;
- (e) data related practices of the provider.

The assessments shall also analyse whether and how the risks pursuant to paragraph 1 are influenced by intentional manipulation of their service, including by inauthentic use or automated exploitation of the service, as well as the amplification and potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions.

The assessment shall take into account specific regional or linguistic aspects, including when specific to a Member State.

3. Providers of very large online platforms and of very large online search engines shall preserve the supporting documents of the risk assessments for at least three years after the performance of risk assessments, and shall, upon request, communicate them to the Commission and to the Digital Services Coordinator of establishment.

Article 35

Mitigation of risks

1. Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable:

- (a) adapting the design, features or functioning of their services, including their online interfaces;
- (b) adapting their terms and conditions and their enforcement;
- (c) adapting content moderation processes, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular in respect of illegal hate speech or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation;
- (d) testing and adapting their algorithmic systems, including their recommender systems;
- (e) adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide;
- (f) reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk;
- (g) initiating or adjusting cooperation with trusted flaggers in accordance with Article 22 and the implementation of the decisions of out-of-court dispute settlement bodies pursuant to Article 21;
- (h) initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively;
- (i) taking awareness-raising measures and adapting their online interface in order to give recipients of the service more information;
- (j) taking targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate;
- (k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information.

2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year. The reports shall include the following:

- (a) identification and assessment of the most prominent and recurrent systemic risks reported by providers of very large online platforms and of very large online search engines or identified through other information sources, in particular those provided in compliance with Articles 39, 40 and 42;

3. As regards paragraph 2, points (a), (b) and (c), where a provider of very large online platform or of very large online search engine has removed or disabled access to a specific advertisement based on alleged illegality or incompatibility with its terms and conditions, the repository shall not include the information referred to in those points. In such case, the repository shall include, for the specific advertisement concerned, the information referred to in Article 17(3), points (a) to (e), or Article 9(2), point (a)(i), as applicable.

The Commission may, after consultation of the Board, the relevant vetted researchers referred to in Article 40 and the public, issue guidelines on the structure, organisation and functionalities of the repositories referred to in this Article.

Article 40

Data access and scrutiny

1. Providers of very large online platforms or of very large online search engines shall provide the Digital Services Coordinator of establishment or the Commission, at their reasoned request and within a reasonable period specified in that request, access to data that are necessary to monitor and assess compliance with this Regulation.

2. Digital Services Coordinators and the Commission shall use the data accessed pursuant to paragraph 1 only for the purpose of monitoring and assessing compliance with this Regulation and shall take due account of the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of personal data, the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

3. For the purposes of paragraph 1, providers of very large online platforms or of very large online search engines shall, at the request of either the Digital Service Coordinator of establishment or of the Commission, explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems.

4. Upon a reasoned request from the Digital Services Coordinator of establishment, providers of very large online platforms or of very large online search engines shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraph 8 of this Article, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union, as set out pursuant to Article 34(1), and to the assessment of the adequacy, efficiency and impacts of the risk mitigation measures pursuant to Article 35.

5. Within 15 days following receipt of a request as referred to in paragraph 4, providers of very large online platforms or of very large online search engines may request the Digital Services Coordinator of establishment, to amend the request, where they consider that they are unable to give access to the data requested because one of following two reasons:

- (a) they do not have access to the data;
- (b) giving access to the data will lead to significant vulnerabilities in the security of their service or the protection of confidential information, in particular trade secrets.

6. Requests for amendment pursuant to paragraph 5 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.

The Digital Services Coordinator of establishment shall decide on the request for amendment within 15 days and communicate to the provider of the very large online platform or of the very large online search engine its decision and, where relevant, the amended request and the new period to comply with the request.

7. Providers of very large online platforms or of very large online search engines shall facilitate and provide access to data pursuant to paragraphs 1 and 4 through appropriate interfaces specified in the request, including online databases or application programming interfaces.

8. Upon a duly substantiated application from researchers, the Digital Services Coordinator of establishment shall grant such researchers the status of 'vetted researchers' for the specific research referred to in the application and issue a reasoned request for data access to a provider of very large online platform or of very large online search engine pursuant to paragraph 4, where the researchers demonstrate that they meet all of the following conditions:

- (a) they are affiliated to a research organisation as defined in Article 2, point (1), of Directive (EU) 2019/790;
- (b) they are independent from commercial interests;
- (c) their application discloses the funding of the research;
- (d) they are capable of fulfilling the specific data security and confidentiality requirements corresponding to each request and to protect personal data, and they describe in their request the appropriate technical and organisational measures that they have put in place to this end;
- (e) their application demonstrates that their access to the data and the time frames requested are necessary for, and proportionate to, the purposes of their research, and that the expected results of that research will contribute to the purposes laid down in paragraph 4;
- (f) the planned research activities will be carried out for the purposes laid down in paragraph 4;
- (g) they have committed themselves to making their research results publicly available free of charge, within a reasonable period after the completion of the research, subject to the rights and interests of the recipients of the service concerned, in accordance with Regulation (EU) 2016/679.

Upon receipt of the application pursuant to this paragraph, the Digital Services Coordinator of establishment shall inform the Commission and the Board.

9. Researchers may also submit their application to the Digital Services Coordinator of the Member State of the research organisation to which they are affiliated. Upon receipt of the application pursuant to this paragraph the Digital Services Coordinator shall conduct an initial assessment as to whether the respective researchers meet all of the conditions set out in paragraph 8. The respective Digital Services Coordinator shall subsequently send the application, together with the supporting documents submitted by the respective researchers and the initial assessment, to the Digital Services Coordinator of establishment. The Digital Services Coordinator of establishment shall take a decision whether to award a researcher the status of 'vetted researcher' without undue delay.

While taking due account of the initial assessment provided, the final decision to award a researcher the status of 'vetted researcher' lies within the competence of Digital Services Coordinator of establishment, pursuant to paragraph 8.

10. The Digital Services Coordinator that awarded the status of vetted researcher and issued the reasoned request for data access to the providers of very large online platforms or of very large online search engines in favour of a vetted researcher shall issue a decision terminating the access if it determines, following an investigation either on its own initiative or on the basis of information received from third parties, that the vetted researcher no longer meets the conditions set out in paragraph 8, and shall inform the provider of the very large online platform or of the very large online search engine concerned of the decision. Before terminating the access, the Digital Services Coordinator shall allow the vetted researcher to react to the findings of its investigation and to its intention to terminate the access.

11. Digital Services Coordinators of establishment shall communicate to the Board the names and contact information of the natural persons or entities to which they have awarded the status of 'vetted researcher' in accordance with paragraph 8, as well as the purpose of the research in respect of which the application was made or, where they have terminated the access to the data in accordance with paragraph 10, communicate that information to the Board.

12. Providers of very large online platforms or of very large online search engines shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers, including those affiliated to not for profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Article 34(1).

13. The Commission shall, after consulting the Board, adopt delegated acts supplementing this Regulation by laying down the technical conditions under which providers of very large online platforms or of very large online search engines are to share data pursuant to paragraphs 1 and 4 and the purposes for which the data may be used. Those delegated acts shall lay down the specific conditions under which such sharing of data with researchers can take place in compliance with Regulation (EU) 2016/679, as well as relevant objective indicators, procedures and, where necessary, independent advisory mechanisms in support of sharing of data, taking into account the rights and interests of the providers of very large online platforms or of very large online search engines and the recipients of the service concerned, including the protection of confidential information, in particular trade secrets, and maintaining the security of their service.

Article 41

Compliance function

1. Providers of very large online platforms or of very large online search engines shall establish a compliance function, which is independent from their operational functions and composed of one or more compliance officers, including the head of the compliance function. That compliance function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or of the very large online search engine to monitor the compliance of that provider with this Regulation.

2. The management body of the provider of the very large online platform or of the very large online search engine shall ensure that compliance officers have the professional qualifications, knowledge, experience and ability necessary to fulfil the tasks referred to in paragraph 3.

The management body of the provider of the very large online platform or of the very large online search engine shall ensure that the head of the compliance function is an independent senior manager with distinct responsibility for the compliance function.

The head of the compliance function shall report directly to the management body of the provider of the very large online platform or of the very large online search engine, and may raise concerns and warn that body where risks referred to in Article 34 or non-compliance with this Regulation affect or may affect the provider of the very large online platform or of the very large online search engine concerned, without prejudice to the responsibilities of the management body in its supervisory and managerial functions.

The head of the compliance function shall not be removed without prior approval of the management body of the provider of the very large online platform or of the very large online search engine.

3. Compliance officers shall have the following tasks:

- (a) cooperating with the Digital Services Coordinator of establishment and the Commission for the purpose of this Regulation;
- (b) ensuring that all risks referred to in Article 34 are identified and properly reported on and that reasonable, proportionate and effective risk-mitigation measures are taken pursuant to Article 35;
- (c) organising and supervising the activities of the provider of the very large online platform or of the very large online search engine relating to the independent audit pursuant to Article 37;

- (d) informing and advising the management and employees of the provider of the very large online platform or of the very large online search engine about relevant obligations under this Regulation;
- (e) monitoring the compliance of the provider of the very large online platform or of the very large online search engine with its obligations under this Regulation;
- (f) where applicable, monitoring the compliance of the provider of the very large online platform or of the very large online search engine with commitments made under the codes of conduct pursuant to Articles 45 and 46 or the crisis protocols pursuant to Article 48.

4. Providers of very large online platforms or of very large online search engines shall communicate the name and contact details of the head of the compliance function to the Digital Services Coordinator of establishment and to the Commission.

5. The management body of the provider of the very large online platform or of the very large online search engine shall define, oversee and be accountable for the implementation of the provider's governance arrangements that ensure the independence of the compliance function, including the division of responsibilities within the organisation of the provider of very large online platform or of very large online search engine, the prevention of conflicts of interest, and sound management of systemic risks identified pursuant to Article 34.

6. The management body shall approve and review periodically, at least once a year, the strategies and policies for taking up, managing, monitoring and mitigating the risks identified pursuant to Article 34 to which the very large online platform or the very large online search engine is or might be exposed to.

7. The management body shall devote sufficient time to the consideration of the measures related to risk management. It shall be actively involved in the decisions related to risk management, and shall ensure that adequate resources are allocated to the management of the risks identified in accordance with Article 34.

Article 42

Transparency reporting obligations

1. Providers of very large online platforms or of very large online search engines shall publish the reports referred to in Article 15 at the latest by two months from the date of application referred to in Article 33(6), second subparagraph, and thereafter at least every six months.

2. The reports referred to in paragraph 1 of this Article published by providers of very large online platforms shall, in addition to the information referred to in Article 15 and Article 24(1), specify:

- (a) the human resources that the provider of very large online platforms dedicates to content moderation in respect of the service offered in the Union, broken down by each applicable official language of the Member States, including for compliance with the obligations set out in Articles 16 and 22, as well as for compliance with the obligations set out in Article 20;
- (b) the qualifications and linguistic expertise of the persons carrying out the activities referred to in point (a), as well as the training and support given to such staff;
- (c) the indicators of accuracy and related information referred to in Article 15(1), point (e), broken down by each official language of the Member States.

The reports shall be published in at least one of the official languages of the Member States.

3. In addition to the information referred to in Articles 24(2), the providers of very large online platforms or of very large online search engines shall include in the reports referred to in paragraph 1 of this Article the information on the average monthly recipients of the service for each Member State.

4. Providers of very large online platforms or of very large online search engines shall transmit to the Digital Services Coordinator of establishment and the Commission, without undue delay upon completion, and make publicly available at the latest three months after the receipt of each audit report pursuant to Article 37(4):

- (a) a report setting out the results of the risk assessment pursuant to Article 34;
- (b) the specific mitigation measures put in place pursuant to Article 35(1);
- (c) the audit report provided for in Article 37(4);
- (d) the audit implementation report provided for in Article 37(6);
- (e) where applicable, information about the consultations conducted by the provider in support of the risk assessments and design of the risk mitigation measures.

5. Where a provider of very large online platform or of very large online search engine considers that the publication of information pursuant to paragraph 4 might result in the disclosure of confidential information of that provider or of the recipients of the service, cause significant vulnerabilities for the security of its service, undermine public security or harm recipients, the provider may remove such information from the publicly available reports. In that case, the provider shall transmit the complete reports to the Digital Services Coordinator of establishment and the Commission, accompanied by a statement of the reasons for removing the information from the publicly available reports.

Article 43

Supervisory fee

1. The Commission shall charge providers of very large online platforms and of very large online search engines an annual supervisory fee upon their designation pursuant to Article 33.
2. The overall amount of the annual supervisory fees shall cover the estimated costs that the Commission incurs in relation to its supervisory tasks under this Regulation, in particular costs related to the designation pursuant to Article 33, to the set-up, maintenance and operation of the database pursuant to Article 24(5) and to the information sharing system pursuant to Article 85, to referrals pursuant to Article 59, to supporting the Board pursuant to Article 62 and to the supervisory tasks pursuant to Article 56 and Section 4 of Chapter IV.
3. The providers of very large online platforms and of very large online search engines shall be charged annually a supervisory fee for each service for which they have been designated pursuant to Article 33.

The Commission shall adopt implementing acts establishing the amount of the annual supervisory fee in respect of each provider of very large online platform or of very large online search engine. When adopting those implementing acts, the Commission shall apply the methodology laid down in the delegated act referred to in paragraph 4 of this Article and shall respect the principles set out in paragraph 5 of this Article. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 88.

4. The Commission shall adopt delegated acts, in accordance with Article 87, laying down the detailed methodology and procedures for:
 - (a) the determination of the estimated costs referred to in paragraph 2;
 - (b) the determination of the individual annual supervisory fees referred to in paragraph 5, points (b) and (c);
 - (c) the determination of the maximum overall limit defined in paragraph 5, point (c); and
 - (d) the detailed arrangements necessary to make payments.

When adopting those delegated acts, the Commission shall respect the principles set out in paragraph 5 of this Article.

*Article 93***Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. This Regulation shall apply from 17 February 2024.

However, Article 24(2), (3) and (6), Article 33(3) to (6), Article 37(7), Article 40(13), Article 43 and Sections 4, 5 and 6 of Chapter IV shall apply from 16 November 2022.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 19 October 2022.

For the European Parliament

The President

R. METSOLA

For the Council

The President

M. BEK

SCHEDULED FOR ORAL ARGUMENT IN SEPTEMBER 2024

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC.,

and

BYTEDANCE LTD.,

Petitioners,

v.

MERRICK B. GARLAND, in his official
capacity as Attorney General of the United
States,

Respondent.

No. 24-1113

DECLARATION OF RANDAL S. MILCH

JUNE 17, 2024

TABLE OF CONTENTS

I.	Qualifications.....	1
II.	Assignment and Summary of Opinions.....	3
III.	Opinions.....	6
A.	Divestitures of highly integrated assets are complex and time-consuming processes.....	6
B.	Certain divestitures are more complex than others.....	10
C.	A “qualified divestiture” of TikTok’s U.S. application would be highly complex.....	12
D.	Market examples show that complex divestitures are time-consuming processes	18
	1. My experience with Verizon’s divestitures illustrates the time-consuming and complex nature of divesting highly integrated assets	18
	2. Other high-value divestitures in the TMT sector illustrate the length and complexity of divesting highly integrated assets	23
E.	A “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within the timeline required by the Act.....	42

I. QUALIFICATIONS

1. I am a Professor of Practice at New York University (“NYU”) School of Law, where I have taught courses in cybersecurity, hacking, regulation, and corporate governance since 2018. I am a Faculty Director of the NYU Master of Science in Cybersecurity Risk & Strategy Program. I also serve as the co-chair of the NYU Center for Cybersecurity. In these roles, I have developed, and I direct, an academic program that seeks to bridge the gaps between technical and non-technical cybersecurity professionals. Since 2015, I have also been a Distinguished Fellow at the Reiss Center for Law and Security at NYU School of Law. I was previously a lecturer in law at Columbia Business School, where I co-taught a course on public policy and business strategy.

2. Prior to my work at NYU, I was employed for 21 years at Verizon Communications Inc. (“Verizon”) and its corporate predecessor Bell Atlantic.¹ From 2008 to 2014, I served as Verizon’s Executive Vice President, Public Policy, and General Counsel. In that role I was responsible for, among other matters, all state, federal, and international regulatory, public policy, and national security issues at Verizon. Beginning in 2008, I was the senior officer at Verizon holding a Top Secret/Sensitive Compartmented Information security clearance. I received that clearance in 2006, when I began serving as the Senior Vice President and General Counsel of Verizon Business, Verizon’s global enterprise business. From 2000 to 2005, I served as the Senior Vice President and General Counsel of Verizon Telecom, where I

¹ For the remainder of my declaration, I include all of Verizon’s corporate predecessors (including General Telephone & Electronics Corporation, or “GTE”) in the term “Verizon.” Verizon was created by the merger of Bell Atlantic with GTE in 2000. Both parties brought with them their long-held legacy wireline assets. *See* “Bell Atlantic and GTE Complete Their Merger and Become Verizon Communications,” Verizon News Archives, June 30, 2000, <https://www.verizon.com/about/news/press-releases/bell-atlantic-and-gte-complete-their-merger-and-become-verizon-communications>.

was responsible for, among other matters, all state regulatory and public policy issues affecting Verizon's landline businesses in the United States. In the foregoing roles at Verizon, I was involved in the divestiture of numerous assets, as I will describe later in this declaration.

3. From 1997 to 2000, I served as Vice President and Associate General Counsel of Bell Atlantic, where my responsibilities included implementation of all aspects of the 1996 Telecommunications Act, including its competition provisions. This role included developing and litigating the case before the New York Public Service Commission that resulted in Verizon New York being the first Bell company allowed to enter the long distance and enterprise markets. The principal issue in that case concerned the development of software operation support systems to interconnect competitors' ordering systems with Bell Atlantic-New York's operations systems. I was, as a result, deeply involved in the requirements for, and testing of, complex software. I joined a Bell Atlantic subsidiary, Bell Atlantic-Maryland, in 1993 as a regulatory attorney.

4. I received my bachelor's degree in American History from Yale University in 1980, and my Juris Doctor (J.D.) from NYU School of Law in 1985. I held a judicial clerkship for the Honorable Clement F. Haynsworth, Jr., in the United States Court of Appeals for the Fourth Circuit. A current copy of my curriculum vitae is included as **Appendix A** to this declaration. I have previously testified under oath before various Committees of Congress, including on national security issues. A list of my unclassified testimony is included in my curriculum vitae.

5. In preparing this declaration, I received research support from individuals at Analysis Group, Inc., a consulting firm, working under my direction and guidance.

6. The sources I have relied upon are cited throughout this declaration. Should additional relevant documents or information be made available to me, I may adjust or supplement my opinions as appropriate.

II. ASSIGNMENT AND SUMMARY OF OPINIONS

7. I have been retained by Counsel for TikTok Inc. and ByteDance Ltd. (together, “Petitioners”)² to evaluate whether a potential divestiture of the integrated global TikTok platform’s (“TikTok”) U.S. application is feasible from an operational perspective within the timeframe and under the restrictions set out in the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”), signed on April 24, 2024.

8. On its face, the Act appears to present Petitioners with a choice: (a) sell TikTok’s U.S. application on terms set out in the Act, or (b) be banned from operating TikTok in the United States. The ban occurs by default under the Act by making it unlawful in the United States to: (1) provide internet hosting services to Petitioners; and (2) distribute mobile applications operated by Petitioners after January 19, 2025 (or, if the President permits, after April 19, 2025).³ Thus, the TikTok application will be banned within the United States after these deadlines unless Petitioners have made a “qualified divestiture” of TikTok’s U.S. application on or before the deadlines.⁴

² “ByteDance Ltd.” is a corporate entity incorporated in the Cayman Islands. “TikTok Inc.” is a corporate entity incorporated in the United States. “TikTok” is an online application that includes the TikTok mobile application and TikTok through a web browser.

³ The Act, Section 2(a)(1).

⁴ The prohibition defined by the Act takes effect on January 19, 2025, which is 270 days after the enactment of the Act (on April 24, 2024). The President may extend this deadline by three months (to April 19, 2025) if a path to a qualified divestiture has been identified or significant progress has been made. The Act, Section 2(a)(2)-(3).

9. As I discuss below, it is my opinion that the divestiture option is entirely illusory and that the Act in fact imposes a ban on TikTok’s U.S. application after the relevant deadlines.⁵ Because a “qualified divestiture” under the Act is one in which the TikTok application operated in the United States cannot have “any operational relationship” with Petitioners,⁶ it is my opinion that a “qualified divestiture” of TikTok’s U.S. application would not be operationally feasible by January (or even April) 2025. I base my opinion on my: (1) review of relevant literature, (2) review of information about TikTok, (3) experience with complex divestitures of highly integrated assets, and (4) evaluation of publicly available information on divestitures in the technology, media, and telecommunications (“TMT”) sector.

10. As I explain below, divestitures of highly integrated assets are complex and time-consuming processes. Sellers and buyers of divested assets must undertake two efforts. The first effort can be thought of as comprising “corporate” steps, such as negotiations between buyer and seller, the signing of a definitive agreement between the parties, seeking regulatory approval for the deal, and the closing of the transaction. The second effort (which may partially overlap with the first) involves “operational” steps, which generally entail planning for and executing the

⁵ I have been instructed by Counsel to assume that the asset to be divested in any qualified divestiture would be the TikTok U.S. application, as opposed to discrete assets of the TikTok business. For this reason, I have not analyzed the timelines associated with theoretical options of a buyer acquiring only parts of TikTok’s U.S. application or buying the application with the intention to engage in asset stripping, such as by liquidating any real estate assets or monetizing solely its user list data. I understand that Counsel’s interpretation is consistent with the language of the Act, which contemplates the qualified divestiture of the TikTok “application,” as well as statements from congressional sponsors. Rep. Krishnamoorthi, for example, has stated: “This particular bill ensures that ByteDance divests itself of the vast majority of the ownership of TikTok. Our intention is for TikTok to continue to operate [...]” “House Debate on H.R. 7521, H1163-1171,” Congressional Record — House, March 13, 2024, <https://www.congress.gov/118/crec/2024/03/13/170/45/CREC-2024-03-13-pt1-PgH1163-2.pdf>.

⁶ The Act “precludes the establishment or maintenance of any operational relationship between the United States operations of the relevant foreign adversary controlled application and any formerly affiliated entities that are controlled by a foreign adversary, including any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing.” The Act, Section 2(g)(6)(B).

carve-out of the financial, personnel, physical, and software assets that will be divested with the business.

11. These operational steps, particularly in complex divestitures of highly integrated assets, take a considerable length of time.⁷ In each example of complex divestitures of highly integrated assets that I evaluated, the operational timeline was much longer than the 270 (or 360) days afforded to Petitioners under the Act. Because the Act precludes the buyer from having “any operational relationship” with Petitioners as of the statutory deadline, all operational steps must be completed before the applicable deadline for the divestiture to satisfy the definition of a “qualified divestiture.”⁸

12. The complexity of a divestiture—and thus the amount of time it takes to achieve, all else equal—increases if there is a high level of integration (*i.e.*, the extent to which complex systems are shared) between the divested asset and the rest of the seller’s company. The information I reviewed regarding a potential divestiture of TikTok’s U.S. application suggests that achieving a “qualified divestiture” would be highly complex given, among other potential factors, the high level of integration between TikTok’s U.S. application and the global TikTok application. As I describe in **Section III.C**, this remains the case notwithstanding the technological and governance protections on which Petitioners have been working.⁹

13. My experience with facilitating complex divestitures at Verizon shows that divesting highly integrated assets to the point where the seller has no operational relationship takes much longer than the time afforded to Petitioners in the Act (in the Verizon examples,

⁷ As I describe below in **Section III.A**, the corporate timeline can also take hundreds of days. I have made the conservative assumption in my declaration that Petitioners could achieve a corporate timeline of zero days.

⁸ The Act, Section 2(g)(6)(B).

⁹ See paragraph 29 for a discussion of “Project Texas.”

approximately twice as long as the time afforded to Petitioners). My personal experience is corroborated by my evaluation of the operational timelines associated with the divestitures of certain highly integrated assets in the TMT sector.

14. For the above reasons and as further explained below, it is my opinion that achieving a “qualified divestiture” of TikTok’s U.S. application is operationally infeasible within the timeframe and under the restrictions set out in the Act. Therefore, the Act offers no real alternative to Petitioners and instead amounts to a *de facto* ban on the TikTok application in the United States starting on January (or April) 19, 2025.

III. OPINIONS

A. Divestitures of highly integrated assets are complex and time-consuming processes

15. Divestitures—the partial or full disposal of a company’s business unit, division, subsidiary, product line, or other assets—are complex undertakings.¹⁰ As I described above, in addition to “corporate” steps, companies must also undertake “operational” steps. As shown in **Figure 1**, when divesting integrated assets, the operational timeline begins when the parties start discussing the mechanics of the transition (which may occur before or after signing the deal) and

¹⁰ Joy, Joseph (2018), *Divestitures and Spin-Offs: Lessons Learned in the Trenches of the World’s Largest M&A Deals* (1st ed. 2018), Springer US (“Joy 2018”), p. 457 (“Divestitures are complex endeavors”). *See also* Joshi, Varun and Sharma, Saurav (2013), Chapter 1 Introduction to the IT Aspects of Mergers, Acquisitions, and Divestitures, In J. M. Roehl-Anderson (Ed.), *M&A Information Technology Best Practices* (pp. 1-22), Wiley (“Joshi 2013”), p. 14 (“Identifying and carving out the pieces in a divestiture can be a complex and time-consuming process”). I include within my definition of “divestitures” spinoffs (*i.e.*, “a type of divestiture in which the divested unit becomes an independent company instead of being sold to a third party”) and splitoffs (*i.e.*, divestitures similar to spinoffs where the shareholders “relinquish their shares of stock in the parent company in order to receive shares of the subsidiary company”). Lessambo, Felix (2021), Chapter 12 Corporate Divestitures and Carve-Outs, In *U.S. Mergers and Acquisitions* (pp. 159-170), Springer, p. 163; CFI Team, “Spin-Off,” CFI, <https://corporatefinanceinstitute.com/resources/valuation/spin-off-and-split-off/>.

ends when the new owner operates the divested assets without the seller's assistance (which may occur on or after the deal's closing).

Figure 1 - Divestiture Timelines¹¹



16. To this end, prior to closing, buyers often contract with the seller to assist with the post-closing operation of the divested asset, such as by providing access to existing software and associated expertise through Transition Services Agreements (“TSAs”) or other similar arrangements.¹² TSAs and similar agreements provide the buyer with access to technology or other support after closing to maintain business continuity.¹³ However, TSAs and similar agreements are far from ideal for either the buyer or the seller.¹⁴ For example, by relying on the seller to provide key technology services to the buyer, the buyer loses direct control over its newly acquired systems and can face increased security risks. Similarly, the seller is often

¹¹ Adapted from Joy 2018, p. 186, based on my professional experience.

¹² Joy 2018, pp. 374, 451-453.

¹³ Joy 2018, pp. 374, 451-453. *See also* Joshi 2013, p. 14 (“Depending on the strategy [from financial close to full separation/exit], it may be beneficial for certain services to be covered under a [TSA]. A TSA is a legal agreement, separate from the separation and purchase agreement, in which the buyer agrees to pay the seller for certain services to support the divested business for a defined period of time. TSAs are most often used in carve-outs where the buyer lacks the necessary information technology capabilities or capacity to support the business on its own. [...] TSAs are also often necessary when the deal closes faster than the buyer’s organization can respond.”).

¹⁴ Joy 2018, pp. 34, 433.

obliged by the service agreement to direct its resources to provide services to the buyer, which diverts resources away from the seller's core business.¹⁵ Therefore, both parties typically seek to keep the length of transition services as short as possible.

17. Importantly, because the Act precludes a buyer of TikTok's U.S. application from having "any operational relationship" with Petitioners after January (or April) 2025,¹⁶ the Act effectively limits the entire timeline (corporate and operational) to 270 (or perhaps 360) days.¹⁷

18. As my analysis below shows, the corporate timeline—which primarily affords the parties the time to analyze and negotiate the allocation of deal risks between them¹⁸—can take hundreds of days.¹⁹ However, because the parties can control certain basic elements of the corporate timeline, the parties may decide to accelerate this timeline (by, for instance, foregoing some risk mitigation steps, such as due diligence).²⁰ In contrast, the parties typically cannot

¹⁵ Joy 2018, pp. 34, 433.

¹⁶ The Act, Section 2(g)(6)(B).

¹⁷ I note that, from the day of submitting my declaration on June 20, 2024, Petitioners have only 214 days left until January 19, 2025; and they have only 304 days left until April 19, 2025. Nevertheless, throughout my declaration, to be conservative, I use 270 and 360 days as the operative figures.

¹⁸ Jacob Orosz, "The M&A Purchase Agreement | An Overview," Morgan & Westfield, <https://morganandwestfield.com/knowledge/purchase-agreement/> ("The purchase agreement can also be seen as a tool for allocating risk between buyer and seller.").

¹⁹ The corporate steps include, among other things: identifying the divestment approach (*e.g.*, through a spin-off or a carve-out); identifying the buyer; defining the divestiture strategy; addressing legal, financial, human resources, and information technology considerations; signing; and closing. These steps generally take a considerable amount of time. *See, for example:* Richard D. Harroch, David A. Lipkin, and Richard V. Smith, "What You Need To Know About Mergers & Acquisitions: 12 Key Considerations When Selling Your Company," *Forbes*, August 27, 2018, <https://www.forbes.com/sites/allbusiness/2018/08/27/mergers-and-acquisitions-key-considerations-when-selling-your-company/?sh=2ef58cd84102>; Jens Kengelbach, Alexander Roos, and Georg Keienburg, "Maximizing Value: Choose the Right Exit Route," BCG, September 22, 2014, <https://www.bcg.com/publications/2014/mergers-acquisitions-divestitures-maximizing-value>; Joy 2018, pp. 26-28.

²⁰ In some cases, divestitures also require the approval of regulatory authorities, such as the Federal Trade Commission or the Federal Communications Commission. A detailed study of recent transactions shows that seeking regulatory approval can delay the transaction by "three to six months [...], but more complicated deals often take twice as long, up to two years." (*See* Suzanne Kumar, Adam Haller, and Dale Stafford, "Regulation and M&A: How Scrutiny Raises the Bar for Acquirers," Bain & Company, January 30, 2024,

meaningfully accelerate the operational timeline. This is because—due to the need to continue operating the divested assets—operational steps cannot be accomplished in less time than the time required for employees to plan and execute the “physical separation of the [...] IT infrastructure, applications, and data, from the divesting company,” which “often includes separating data and processes within legacy IT systems that were not designed or built to enable future decoupling.”²¹ The common utilization of TSAs, which as noted are not ideal for either party, demonstrates that operational timelines cannot be meaningfully compressed despite economic incentives to do so.

19. Because the parties can control certain basic elements of the corporate timeline, I have made the conservative assumption in my declaration that Petitioners could achieve a corporate timeline of zero days. However, even assuming Petitioners could have instantaneously negotiated a divestiture agreement on the day the Act was signed into law, they still could not achieve a qualified divestiture within the timeline allowed by the Act: as I show below, the

<https://www.bain.com/insights/regulation-m-and-a-report-2024/>.) Regulatory delays are typically not in the parties’ control. Because regulatory delays are part of the corporate timeline, and my analysis focuses on operational timelines, my analysis does not include the time required to achieve regulatory approvals.

²¹ Philip W. Yetton et al., “How IT Carve-Out Project Complexity Influences Divestor Performance in M&As,” *European Journal of Information Systems*, Vol. 32, No. 6, 2023, pp. 962-988 (“Yetton 2023”), at p. 965. *See also* Yetton 2023, at p. 964 (“[T]he timeframe in the contract is frequently too tight to execute the required IT carve-out. In that case, Operational Day 1 represents an operationally viable *intermediate IT-state* [emphasis in original] in which the provision of IT services by the divestor is formally enabled by TSAs. [...] TSAs are attractive because they make an earlier Operational Day 1 possible and provide reliable IT support until Physical IT Separation.”); at p. 976 (“[W]ith increasing project complexity, the transfer of IT assets to the acquirer is incompatible with the set Operational Day 1 [...]. The time constraint contingent on satisfying Operational Day 1 readiness is particularly problematic in the context of IT carve-out projects because the time constraint on the project is not based on an estimate of the time required for the project but set by market expectations for the acquirer to realise [sic] acquisition benefits.”). *See also* Joshi 2013, p. 10 (“[Day 1] requirements should be highly focused on keeping the business running, removing uncertainty for stakeholders, complying with regulatory requirements, and delivering the Day 1 must-haves”); Kin, Blair (2013), Chapter 21 Planning for Business Process Changes Impacting Information Technology, In J. M. Roehl-Anderson (Ed.), *M&A Information Technology Best Practices* (pp. 376-377), Wiley, pp. 376-377 (“[t]he IT staff will need to have a full understanding of what functions will remain in use so the proper changes can be made. This effort is time-consuming for the IT staff that is already engaged in changes to other complicated post-merger integrations.”).

operational timelines alone of divestitures with similar levels of integration as TikTok took longer than 360 days (let alone 270 days).

B. Certain divestitures are more complex than others

20. While I would consider any divestiture a complex undertaking, there is a range of complexity, and certain divestitures are more complex than others. Academic and industry participants have identified specific characteristics that affect the complexity of a divestiture. For example, the Divestiture Complexity Assessment (“DCA”) Framework considers, among other factors, the following two key factors when gauging the complexity of a planned divestiture.²²

- a) **The level of integration**, *i.e.*, the extent to which the divested asset and the rest of the seller share information technology (“IT”) systems and applications, and the ease with which the seller can separate these systems and applications.²³ The greater the level of integration, the more complex the divestiture because the “IT function [is] the most complex function to separate.”²⁴
- b) **Post-divestiture support from the seller**, *i.e.*, whether the seller will provide support to the divested asset in the form of TSAs or other arrangements after the

²² Joy 2018, pp. 17-18.

²³ The DCA framework uses the term “comingling” [sic] for integration. Joy 2018, pp. 17-18.

²⁴ Joy 2018, p. 12. *See also* Yetton 2023, at p. 965 (“IT carve-out projects are frequently complex, accounting for more than 50% of the overall carve-out cost”); Joshi 2013, p. 14 (“Identifying and carving out the pieces in a divestiture can be a complex and time-consuming process, particularly when the affected people, processes, and systems are deeply integrated within the seller’s business, or when services and infrastructure are shared across multiple business units”); p. 5 (“IT-related activities are generally the largest cost items in a merger or divestiture”); p. 20 (“IT integrations or separations are generally complex, resource-intensive initiatives that need to be closely aligned with the overall business integration effort”).

divestiture.²⁵ Divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing.²⁶

21. The importance of these factors in gauging the expected complexity of a divestiture is consistent with my professional experience in facilitating complex divestitures of highly integrated assets. While other factors certainly play a role in the complexity of a divestiture (such as creating a separate financial framework for the divested asset, and dealing with employee matters), based on my experience the above two factors are particularly relevant in determining complexity.

22. As I describe in the following sections, I have evaluated historical divestitures and the “qualified divestiture” the Act requires from Petitioners along the following dimensions.

- a. To capture the extent of “integration” and the ease with which the divested asset could be separated from the rest of the seller, I evaluated the following:
 - i. Whether the divested asset can be separated from the rest of the seller based solely on product market.²⁷ If that is the case, isolating the divested

²⁵ The DCA framework uses the term “Health of the seller company” for post-divestiture support from the seller. *See* Joy 2018, p. 18 (“How is the health of the seller company? Will it be able to provide support to the buyer in form of TSAs post-divestiture? Is there any dependency on the seller company post-divestiture?”).

²⁶ *See, e.g.*, Joshi 2013, p. 14 (“TSAs are most often used in carve-outs where the buyer lacks the necessary information technology capabilities or capacity to support the business on its own. [...] TSAs are also often necessary when the deal closes faster than the buyer’s organization can respond.”).

²⁷ A divested asset can be defined based solely on product market if geographic considerations are not necessary to define the asset. For example, if a company divests its software business in Canada while continuing to operate the same business in the United States, this divestiture is not defined based solely on product market. However, if a company divests its entire software business (regardless of geography), while retaining its hardware business, this divestiture is defined based solely on product market.

asset is simpler than if the divestiture involves separating one or more products into multiple pieces based on geographic market.

- ii. Whether the seller acquired the divested asset within ten years of the evaluated divestiture. This fact suggests a more limited level of “integration” of the divested asset with the rest of the seller than if the seller had developed the divested asset organically or if the seller had acquired it more than ten years before the evaluated divestiture.²⁸

- b. I also evaluated whether the deal included a TSA or a similar agreement that indicates ongoing technical support from the seller after the deal closed.²⁹

C. A “qualified divestiture” of TikTok’s U.S. application would be highly complex

23. While the details of a potential “qualified divestiture” of TikTok’s U.S. application are currently unknowable, the information that I have reviewed indicates that any “qualified divestiture” of the U.S. application would be highly complex.

24. First, TikTok’s U.S. application and global application are highly integrated. TikTok’s U.S. application offers the same product as TikTok’s global application—that is, the asset to be divested would be defined only by a geographic market, even though the asset is part

²⁸ I use the ten-year benchmark as a proxy for an expected level of integration between an acquired asset and the acquirer. Based on my experience, all else equal, companies have an economic incentive to integrate operations over time. As I describe below, my conclusions would not change even if the threshold were different. First, none of the divestitures I evaluated in **Section III.D** had indicia of being non-complex based on the ten-year acquisition criterion alone. Second, none of the divestitures I evaluated in **Section III.D** took fewer than 270 days.

²⁹ As I discuss in **Section III.D**, public companies and companies in regulated industries frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps.

of a global platform and product. Further, TikTok’s U.S. application is an organic part of TikTok’s global platform; Petitioners did not acquire “TikTok U.S.”³⁰ Indeed, the Draft National Security Agreement (“NSA”) defines the “TikTok U.S. Application” as “all versions of the TikTok Global App provided to, or accessible by, TikTok U.S. Users,”³¹ suggesting that the “TikTok U.S. Application” is indistinguishable from the “TikTok Global App.”

25. Second, the global TikTok application itself is highly integrated with ByteDance.^{32,33} The Harvard Business Review attributes ByteDance’s success in part to its “shared-service platform” model. ByteDance has centralized many technology, operating, and business functions into “shared-service platforms” that can be flexibly deployed to handle many

³⁰ ByteDance’s 2017 acquisition of Musical.ly is irrelevant for this evaluation because divesting TikTok’s U.S. application would be far different than unwinding the Musical.ly transaction. Although ByteDance initially ran Musical.ly as an “independent platform” (“China’s ByteDance Buying Lip-Sync App Musical.ly for Up to \$1 Billion,” Reuters, November 10, 2017, <https://www.reuters.com/article/idUSKBN1DA0BQ/>), before relaunching TikTok in the United States in August 2018, ByteDance “abandoned the Musical.ly code base and technology, including Musical.ly’s recommendation engine, operation system, user growth, and marketing tools.” (Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10.) ByteDance integrated Musical.ly’s “user base, some music licensing agreements and other copyright agreements” with the “technology platform [...] developed by ByteDance before the Musical.ly acquisition had even occurred.” (See Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10. See also Rebecca Fannin, “The Strategy Behind TikTok’s Global Rise,” Harvard Business Review, September 13, 2019, <https://hbr.org/2019/09/the-strategy-behind-tiktoks-global-rise>.) As a result, the current TikTok app in the United States has only the barest attributes of the Musical.ly app from 2017 and there is essentially no Musical.ly app to divest.

³¹ Draft National Security Agreement by and Among: (i) ByteDance Ltd., (ii) TikTok Ltd., (iii) TikTok Inc., and (iv) CFIUS Monitoring Agencies, on behalf of the CFIUS, August 23, 2022.

³² Kane Wu and Julie Zhu, “Exclusive: ByteDance Prefers TikTok Shutdown in US if Legal Options Fail, Sources Say,” Reuters, April 26, 2024, <https://www.reuters.com/technology/bytedance-prefers-tiktok-shutdown-us-if-legal-options-fail-sources-say-2024-04-25/> (“The algorithms TikTok relies on for its operations are deemed core to ByteDance’s overall operations. [...] TikTok shares the same core algorithms with ByteDance domestic apps like short video platform Douyin.”). By ByteDance I mean to refer to the general corporate group, as opposed to any particular corporate entity.

³³ Counsel instructed me to evaluate whether a “qualified divestiture” of TikTok’s U.S. application, as opposed to TikTok’s global application, would be operationally feasible within the timeframe and under the restrictions set out in the Act. That noted, my opinions set out in this declaration would not change if I were to evaluate a “qualified divestiture” of TikTok’s global application. This is because, as I describe in this section, such a divestiture would remain a complicated geographic splitting of a highly integrated product: in this case, the integration of the global TikTok application with ByteDance.

tasks across products—including core engineering tasks.³⁴ The Harvard Business Review’s description of the “shared-service platform” across ByteDance’s products is consistent with Petitioners’ submission to the Committee on Foreign Investment in the United States (“CFIUS”) in August 2021, explaining that the TikTok application (and ByteDance’s other applications) are composed of thousands of “microservices,”³⁵ whereby “small, self-contained teams” can separately develop the software for each service.³⁶ This approach allows product engineering teams to rapidly leverage technologies across products, in effect integrating the software underlying ByteDance’s various apps.^{37,38}

26. Third, as I described above, the Act precludes Petitioners from having “any operational relationship” with the buyer after January (or April) 2025.³⁹ Therefore, the Act effectively prohibits TSAs or other post-divestiture support arrangements. This restriction means that the entire timeline (corporate and operational), including all planning, development, and transition implementation must be completed by the deadline, rendering the divestiture more complex.

³⁴ Roger Chen and Rui Ma, “How ByteDance Became the World’s Most Valuable Startup,” Harvard Business Review, February 24, 2022, <https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup> (“In some cases, product teams customize existing technologies that have already been developed by the SSP [or Shared-Service Platform]. Algorithms are a case in point. Product teams at ByteDance work with SSP algorithm engineers to fine-tune their enormously powerful recommendation engines. [...] As expected, because so many capabilities have been centralized into this large SSP, the actual product teams tend to be small and focused”).

³⁵ CFIUS Questions for ByteDance/TikTok, August 26, 2021, p. 13.

³⁶ “What Are Microservices?,” AWS, <https://aws.amazon.com/microservices/>.

³⁷ Roger Chen and Rui Ma, “How ByteDance Became the World’s Most Valuable Startup,” Harvard Business Review, February 24, 2022, <https://hbr.org/2022/02/how-bytedance-became-the-worlds-most-valuable-startup>.

³⁸ Although ByteDance has provided information to CFIUS regarding the changes that it has made to its software development process since 2021 as part of Project Texas, these changes do not alter my opinion regarding the high level of integration and complexity of a “qualified divestiture” of TikTok’s U.S. application. *See* paragraph 29 for additional information.

³⁹ The Act, Section 2(g)(6)(B).

27. Fourth, according to Petitioners, Chinese export control laws would forbid the divestment of certain elements of TikTok’s integrated software, including in particular its recommendation engine.⁴⁰ According to information provided by Petitioners to CFIUS, as of October 2022, TikTok’s global application consisted of roughly 2 billion lines of code.⁴¹ According to public reports, this length of code is on the same scale as Google was in 2015.⁴² Similarly, according to Petitioners, as of August 2021, there were approximately 4,000 software engineers working on the global TikTok application (with only about 800 of them located in the United States).⁴³ The total number of 4,000 engineers is on the same scale as Uber.⁴⁴ To the extent that—as the result of an export ban—the buyer would need to recreate elements of TikTok’s software before January (or April) 19, 2025, TikTok’s large scale further adds to the complexity of the divestiture. Based on the Act, after the deadline, Petitioners would not be allowed to provide the buyer breathing room while the buyer recreates this infrastructure (*e.g.*, the buyer would not be allowed to run TikTok on the old code while the new code was being created).⁴⁵

⁴⁰ See Letter from Michael E. Leiter, et al., to David Newman (Principal Deputy Assistant Attorney General for National Security), April 1, 2024, pp. 1-2.

⁴¹ “TikTok Source Code Update,” October 24, 2022.

⁴² Cade Metz, “Google Is 2 Billion Lines of Code—And It’s All in One Place,” WIRED, September 16, 2015, <https://www.wired.com/2015/09/google-2-billion-lines-codeand-one-place/> (“So, building Google is roughly the equivalent of building the Windows operating system 40 times over. The [...] 2 billion lines that drive Google are *one thing*.”).

⁴³ CFIUS Questions for ByteDance/TikTok, August 26, 2021, pp. 13-14.

⁴⁴ See “Devpod: Improving Developer Productivity at Uber with Remote Development,” Uber, December 13, 2022, <https://www.uber.com/blog/devpod-improving-developer-productivity-at-uber/> (“Uber’s developer platform serves 5000 core software engineers to build, deploy, and manage high-quality software productively and at scale.”).

⁴⁵ As I described in paragraph 20, divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing. See also Eduardo Cuomo, “What Is Software Maintenance and Why Is It Important?,” Patagonian, March 22, 2023, <https://patagonian.com/blog/what-is-software-maintenance-and-why-is-it-important/> (“Cuomo, 2023”).

28. Fifth, even if Chinese export control laws did not forbid the divestment of certain elements of TikTok’s software, the preclusion of “any operational relationship” between Petitioners and the buyer means that the buyer must, upon divestiture, be prepared to engage in the “ongoing process” of “modifying, upgrading, and updating” the code underlying TikTok’s U.S. application without any post-divestiture support from Petitioners.⁴⁶ As I described above, Petitioners provided information to CFIUS indicating that TikTok has a large code base and development team,⁴⁷ and that TikTok’s software updates have a “high deployment frequency” with “approximately 1,000 backend service deployments to the TikTok application each day.”⁴⁸ TikTok’s large scale and deployment of frequent updates adds to the complexity of the divestiture because software maintenance—an undertaking “no less important than developing the software itself”—is an operational requirement for business continuity that, under the Act, could not be subject to a service agreement after January (or April) 19, 2025.⁴⁹

29. Sixth, my opinion regarding the high level of integration and complexity of a “qualified divestiture” of TikTok’s U.S. application is unchanged by the technological and

⁴⁶ Cuomo, 2023. (“Software development is an ongoing process that requires constant optimization, even after the product is out in the market. [...] Software maintenance involves modifying, upgrading, and updating a software system to solve errors, improve the software itself, increase performance, or adapt the system to a change in conditions or the environment.”).

⁴⁷ See paragraph 27.

⁴⁸ CFIUS Questions for ByteDance/TikTok, August 26, 2021, p. 13. This level of deployments is on the order of Amazon, Google, Netflix, and Facebook. See Cate Lawrence, “Deployment Frequency – A Key Metric in DevOps,” Humanitec, February 4, 2021, <https://humanitec.com/blog/deployment-frequency-key-metric-in-devops> (“[An] elite group [of companies] routinely deploys on-demand and performs multiple deployments per day. [...] Amazon, Google, and Netflix deploy thousands of times per day (aggregated over the hundreds of services that comprise their production environments).”). See also Chuck Rossi, “Continuous Deployment of Mobile Software at Facebook (Showcase),” 2016 24th ACM SIGSOFT International Symposium, November 2016 (“Given the size of Facebook’s engineering team, this resulted in 1,000’s of deployments into production each day.”).

⁴⁹ Cuomo, 2023. As I described in paragraph 20, divestiture processes become more complex when the seller is less able (or willing) to support the divested asset post-divestiture, because if that is the case, the entirety of the operational effort must occur before closing.

governance protections on which Petitioners have been working (dubbed “Project Texas”). I understand that Petitioners have been working on separating U.S. user data from non-U.S. user data, and that certain U.S. user data is stored in a protected enclave in the United States.⁵⁰ As part of Project Texas, ByteDance has established a special purpose subsidiary (TikTok U.S. Data Security Inc.) intended to (1) manage “all business functions that require access to U.S. user data identified by the U.S. government” and (2) safeguard “systems that deliver content on the app in the U.S. to ensure that it is free from foreign manipulation.”⁵¹ However, I understand that neither TikTok U.S. Data Security Inc., nor any other technological and governance protections, have been intended to achieve a complete severing of all “operational relationships” between TikTok’s U.S. application and its global application.⁵² I further understand that Project Texas does not contemplate the elimination of continued operational cooperation between TikTok’s U.S. application and ByteDance globally. For example, Project Texas contemplates TikTok’s U.S. application’s continued reliance on ByteDance engineers for certain fundamental parts of the code infrastructure that make the application work, including its recommendation engine.⁵³ Rather than duplicating these functions in the United States, Project Texas instead contemplates several layers of protection to validate and ensure the integrity of source code developed outside the United States.⁵⁴

⁵⁰ “About Project Texas,” TikTok U.S. Data Security, <https://usds.tiktok.com/usds-about/> (“About Project Texas”).

⁵¹ “About Project Texas”.

⁵² “National Security Agreement CFIUS Case 20-100 Presentation to the Committee on Foreign Investment in the United States,” ByteDance/TikTok, September 8, 2023, (“NSA Presentation, 2023”), p. 16. *See also* “About Project Texas” *and* Matt Perault, “Has TikTok Implemented Project Texas?,” Lawfare, May 10, 2024, <https://www.lawfaremedia.org/article/has-tiktok-implemented-project-texas> (“Perault, 2024”).

⁵³ NSA Presentation, 2023, p. 16. *See also* “About Project Texas” *and* Perault, 2024.

⁵⁴ *See* “About Project Texas” *and* Perault, 2024.

30. For the above reasons, it is my opinion that any “qualified divestiture” of TikTok’s U.S. application would be highly complex.

D. Market examples show that complex divestitures are time-consuming processes

31. As I discussed above, the information that I have reviewed regarding a potential divestiture of TikTok’s U.S. application suggests that achieving a “qualified divestiture” would be highly complex. In this section I describe the time that highly complex divestitures take based on my: (1) experience with complex divestitures of highly integrated assets, and (2) evaluation of public information available on divestitures in the TMT sector. These examples indicate that the operational timeline alone of highly complex divestitures takes more than 360 days, *i.e.*, longer than the time afforded to Petitioners in the Act.

1. My experience with Verizon’s divestitures illustrates the time-consuming and complex nature of divesting highly integrated assets

32. The public often does not observe many of the divestiture steps that buyers and sellers conduct. For strategic reasons, companies often disclose information about a potential divestiture only after the parties have signed a binding agreement (and sometimes only after deal closing).⁵⁵ Similarly, the parties often do not disclose details regarding TSAs or other transition

⁵⁵ Zachary Turke and Edward Xia, “Why It’s Important to Manage Confidentiality in M&A Deals,” *Los Angeles & San Francisco Daily Journal*, August 31, 2020, https://www.sheppardmullin.com/media/publication/1888_Sheppard%20DJ-8-31-2020_.pdf, p. 1 (“Maintaining confidentiality of any information you disclose, including that a potential transaction might occur at all, is of the utmost importance.”).

agreements unless required to do so by law.⁵⁶ Therefore, the public typically only observes the divestiture timeline from the signing of a binding agreement until the close of the deal.

33. Companies in regulated industries, however, frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps. Public records in regulated industries provide detail on the time and work that divestitures require and the associated complexity in the months and years after the divestiture.

34. Accordingly, my experience with three complex divestitures at Verizon, which operates in a regulated industry, allows me to describe comprehensively the time needed to separate and divest a highly integrated asset. These three Verizon divestitures, which I discuss below, illustrate the time-consuming and unpredictable nature of divesting highly integrated assets and the frequent provision of post-closing operational assistance by the seller to the buyer, irrespective of whether the buyer intends to integrate the divested assets into its existing business or to operate a new, stand-alone business.

35. These Verizon examples are relevant to evaluating any potential “qualified divestiture” of TikTok’s U.S. application because, pre-divestiture, the divested assets were highly integrated with the non-divested assets, as is the case between TikTok’s U.S. and global applications. Specifically:

- a. All three Verizon divestitures involved a geographic separation of a portion of Verizon’s business, instead of a more straightforward separation based on product

⁵⁶ As I discuss in **Section III.D**, public companies and companies in regulated industries frequently face obligations to disclose details regarding their divestitures, providing transparency into otherwise concealed divestiture steps.

market alone. Likewise, the divestiture required from Petitioners is a geographic separation of a portion of TikTok's business.

- b. These assets had been highly integrated in Verizon's overall business from a business-process perspective.⁵⁷ Likewise, TikTok's U.S. application is an organic part of TikTok's global application, meaning that the U.S. application is highly integrated in the global application.

36. The total timelines (inclusive of all corporate and operational steps) for these three Verizon divestitures took at least 751 days, 757 days, and 1,056 days, respectively—*i.e.*, each took between two and three times as long as the maximum timeline the Act affords Petitioners.⁵⁸ Importantly, the publicly observable operational timelines alone took at least 422, 727, and 642 days—all well over the time allotted to Petitioners by the Act. I summarize these Verizon divestitures below and provide more detail in **Appendix B**.

37. A 2005 divestiture of Verizon's telephone access lines in Hawaii ("HawaiianTel") spanned a total of 751 days between Verizon's disclosure of deal discussions and the final operational cutover (*i.e.*, the date at which new stand-alone systems were up and running).⁵⁹ Furthermore, the operational timeline alone spanned at least 422 days—that is, longer than the

⁵⁷ See **Exhibit 1** and **Appendix B**.

⁵⁸ A total timeline of 751 days or 757 days is more than two times as long as the maximum timeline the Act affords to Petitioners ($751 \text{ days} / 360 \text{ days} = 2.1$; similarly, $757 \text{ days} / 360 \text{ days} = 2.1$). A total timeline of 1,056 days is nearly three times as long as the maximum timeline the Act affords to Petitioners ($1,056 \text{ days} / 360 \text{ days} = 2.9$).

⁵⁹ The corporate timeline began on March 12, 2004 (when Verizon announced that it had been in divestment discussions), and it ended with the deal closing on May 2, 2005—representing a total of 417 days. See Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2003, p. 15; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2004, p. 16; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7; "Verizon Hawaii, Inc. (GTHI)," Federal Communications Commission, <https://www.fcc.gov/verizon-hawaii-inc-gthi>.

time the Act affords Petitioners, without even considering the incremental corporate timeline.⁶⁰ Verizon and the buyer needed this 422-day period to handle the software challenges of splitting off highly integrated assets and establishing a stand-alone entity. Notably, after the transition began, the parties realized that they had underestimated the complexity of the software transition, and the TSA was extended.⁶¹

38. Similarly, Verizon's 2007 divestiture of its access lines in Maine, Vermont, and New Hampshire (*i.e.*, its Northeast Business), took 757 days between signing of the agreement and the final operational cutover.⁶² The operational timeline alone took at least 727 days.⁶³

⁶⁰ The operational timeline began on February 4, 2005, with the buyer's hiring of BearingPoint to create the necessary back-office systems for a new, stand-alone HawaiianTel and ended on April 1, 2006, when the final cutover to these systems occurred. *See* Decision and Order No. 21696, *In the Matter of the Application of Paradise Mergersub, Inc., GTE Corporation, Verizon Hawaii Inc., Bell Atlantic Communications, Inc., and Verizon Select Services Inc. for Approval of a Merger Transaction and Related Matters.*, No. 04-0140, <https://files.hawaii.gov/dcca/dca/dno/dno2005/21696.pdf>, p. 20; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, pp. 50-51.

⁶¹ The amendment to the initial agreement, dated December 15, 2005, extended the transition period for an additional 60 days to April 1, 2006. *See* Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7.

⁶² The corporate timeline for this divestiture began on January 15, 2007, with the announcement of a deal between Verizon and FairPoint Communications, an established telecommunications provider, and ended on March 31, 2008, with the closing of the deal. *See* Agreement and Plan of Merger by and Among Verizon Communications Inc., Northern New England Spinco Inc., and FairPoint Communications, Inc., January 15, 2007; Joint Application for Approval of the Transfer of Certain Assets by Verizon New England Inc., Bell Atlantic Communications, Inc., NYNEX Long Distance Company, and Verizon Select Services Inc. and Associated Transactions; FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 2.

⁶³ The operational timeline largely overlapped with the corporate timeline and began on February 14, 2007, 30 days after the agreement was signed, when the planning for the transition started pursuant to the TSAs and Master Services Agreements (MSAs). (*See* Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>, p. 13 (“Within 30 calendar days following the date hereof [January 15, 2007, also when the Agreement and Plan of Merger was signed], the Cutover Planning Committee shall hold its initial meeting to commence planning and preparation for the Buyers to cease using all Transition Services and thereafter.”).) On February 9, 2009, FairPoint completed the cutover process and began operating its new systems independently from the Verizon systems. (*See* FairPoint Communications, Inc., Form 10-K for the Fiscal Year Ended December 31, 2008, pp. 2-3.)

Additionally, in September 2008, 595 days into the operational implementation, the parties realized that they had underestimated the complexity of the software transition, and despite a significant amount of pre-cutover system testing, the TSA services were extended.⁶⁴

39. Lastly, Verizon's 2009 divestiture of operations in 14 states ("14-State Divestiture") to Frontier Communications Corporation ("Frontier") spanned 1,056 days between signing of the agreement and the final operational cutover.⁶⁵ At least 642 days elapsed from deal closing to the final operational cutover, during which time underlying operations support was provided through a replica version of Verizon's software until the operation support was migrated to Frontier's own systems.⁶⁶

40. These three Verizon divestitures illustrate the time-consuming and unpredictable nature of divesting highly integrated assets. In all cases, the operational timelines alone—at least 422, 727, and 642 days—were well over the time allotted to Petitioners by the Act, even if the

⁶⁴ FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 54 ("We expect to continue to require transition services agreement services from Verizon through January 2009, which is beyond the six month period following the closing of the merger, during which we anticipated requiring such services."); *2009 Annual Report*, State of Maine Public Utilities Commission, February 1, 2010, <https://www.maine.gov/mpuc/sites/maine.gov/mpuc/files/inline-files/AR09-FINAL.pdf>, p. 11.

⁶⁵ The corporate timeline for the Frontier divestiture began no later than May 13, 2009, when the parties signed an agreement and ended with the closing of the deal on July 1, 2010. (See Memorandum Opinion and Order, *In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 4; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2010, Note 3; "Verizon Completes Spinoff of Local Exchange Businesses and Related Landline Activities in 14 States," Verizon News Archives, July 1, 2010, <https://www.verizon.com/about/news/press-releases/verizon-completes-spinoff-local-exchange-businesses-and-related-landline-activities-14-states>.) Frontier completed the integration of operations from Verizon in April 2012. (See Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.)

⁶⁶ Frontier completed the integration of operations from Verizon on April 2, 2012. See Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>; Memorandum Opinion and Order, *In the Matter of Applications Filed for the Transfer of Certain Spectrum Licenses and Section 214 Authorizations in the States of Maine, New Hampshire, and Vermont from Verizon Communications Inc. and Its Subsidiaries to FairPoint Communications, Inc.*, WC Docket No. 07-22, January 9, 2008, p. 12.

President were to grant an extension to April 2025. In both the 2007 and 2009 divestitures, the operational time alone that Verizon needed to execute the divestiture nearly doubled the maximum amount of time afforded to Petitioners by the Act.⁶⁷

2. *Other high-value divestitures in the TMT sector illustrate the length and complexity of divesting highly integrated assets*

41. My evaluation of additional divestitures in the TMT sector further corroborates my conclusion that complex divestitures with highly integrated assets take longer than the time the Act affords to Petitioners.⁶⁸ Additionally, as I show below, even divestitures of less integrated assets in this sector often take longer than the time afforded to Petitioners in the Act.

42. I used a two-step process to identify comparable historical divestitures. First, I used S&P Capital IQ Pro—the research division of one of the largest providers of financial information⁶⁹—to identify historical divestiture transactions that satisfied the following criteria:⁷⁰

- a. The divested assets operated in the “interactive media and services,” “application software,” “systems software,” or “integrated telecommunication services” industries;⁷¹

⁶⁷ An operational timeline of 727 days or 642 days is nearly two times as long as the maximum timeline the Act affords to Petitioners (727 days / 360 days = 2.0; similarly, 642 days / 360 days = 1.8).

⁶⁸ As I describe below, S&P Capital IQ Pro classifies TikTok Inc. as part of the “Technology, Media & Telecommunications” sector.

⁶⁹ James Chen, “S&P Capital IQ Definition, Products and Services,” Investopedia, April 30, 2024, <https://www.investopedia.com/terms/c/capital-iq.asp>.

⁷⁰ To identify divestiture transactions in S&P Capital IQ Pro, I used the filter “Transaction Type” to select transactions that were either “M&A - Asset” or “M&A - Spinoff or Splitoff.”

⁷¹ S&P Capital IQ Pro classifies TikTok Inc. as part of the “interactive media and services” industry within the “Technology, Media & Telecommunications” sector. Therefore, I limited my research to transactions that involved divested assets operating in the “interactive media and services” industry as well as other industries within the “Technology, Media & Telecommunications” sector that are related to TikTok. For example, I included the industry that S&P Capital IQ Pro uses to classify ByteDance Ltd (“application software”) and

- b. The transaction (1) took place in the United States,⁷² (2) was announced and completed in the last ten years (between 2014 and 2024),⁷³ and (3) had a total transaction value greater than \$1 billion;⁷⁴ and
- c. At least one of either the buyer or the seller had publicly available Securities and Exchange Commission (“SEC”) filings at the time of the divestiture, and the transaction was subject to regulatory or antitrust approval.⁷⁵

43. Including in the selection criteria that at least one of the parties had publicly available SEC filings and that the transaction was subject to regulatory or antitrust approval allowed me, in most cases, to retrieve relevant information (such as information on TSAs) to determine an operational timeline that might otherwise be concealed from the public. I found 26 divestitures that satisfied the above criteria and I refer to these 26 divestitures as my “market sample.”⁷⁶

industries that are closely related to application software (“systems software” or “integrated telecommunication services”).

⁷² Specifically, in S&P Capital IQ Pro, I used the filter “Transaction Geography” to select “United States.”

⁷³ Specifically, in S&P Capital IQ Pro, I used the filter “Announced Date” to select these dates and the filter “Transaction Status” to require that the transaction was “Completed.”

⁷⁴ Specifically, in S&P Capital IQ Pro, I set the data field “Total Transaction Value (\$M)” to be greater than \$1 billion. I used the \$1 billion cutoff because publicly available information indicates that the TikTok transaction would be over \$1 billion. *See, e.g.*, Dylan Butts, “Kevin O’Leary Wants to Buy TikTok at Up to 90% Discount. Here’s Why,” CNBC, March 22, 2024, <https://www.cnbc.com/2024/03/22/kevin-oleary-on-why-he-wants-to-buy-tiktok-.html>; Brian Fung, “Who Could Buy TikTok?,” CNN Business, April 25, 2024, <https://www.cnn.com/2024/04/25/tech/who-could-buy-tiktok/index.html> (describing a value of \$20 billion to \$30 billion); Natalie Andrews et al., “TikTok Crackdown Shifts Into Overdrive, with Sale or Shutdown on Table,” The Wall Street Journal, March 10, 2024, <https://www.wsj.com/tech/why-the-new-effort-to-ban-tiktok-caught-fire-with-lawmakers-7cd3f980> (describing a price tag “in the hundreds of billions of dollars”). With that said, my results hold even if I lower the cutoff to \$750 million.

⁷⁵ Specifically, in S&P Capital IQ Pro, I used the filter “deal condition” to select transactions that are classified as reporting a divestiture subject to “Regulatory or Antitrust Approval” (*e.g.*, subject to competition authority approval).

⁷⁶ My analysis of these 26 divestitures is presented in **Exhibit 1**.

44. Second, to limit my market sample to transactions that involved divestitures of highly integrated assets, I excluded transactions for which either: (1) the divested asset was defined solely based on product market, or (2) the seller acquired the divested asset within ten years of the evaluated divestiture.⁷⁷ The four divestitures that remained were:

- a. Lumen Technologies Inc.'s ("Lumen") 2022 sale of its local exchange business, valued at \$7.5 billion,⁷⁸ to Apollo Global Management ("Apollo");⁷⁹
- b. Frontier's 2020 sale of some of its operations and assets, valued at \$1.35 billion, to a group of financial investors;⁸⁰

⁷⁷ I described the rationale behind these criteria in **Section III.B**.

⁷⁸ Here and in the remainder of my declaration, I report transaction values as shown by S&P Capital IQ Pro.

⁷⁹ In Lumen's case, geographic considerations were necessary to define the divested asset because Lumen divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. The public record that I have reviewed indicates that Lumen did not acquire the divested asset within ten years before the evaluated divestiture. "Lumen to Sell Local Incumbent Carrier Operations in 20 States to Apollo Funds for \$7.5 Billion," PR Newswire, August 3, 2021, <https://www.prnewswire.com/news-releases/lumen-to-sell-local-incumbent-carrier-operations-in-20-states-to-apollo-funds-for-7-5-billion-301347625.html>.

⁸⁰ In Frontier's case, geographic considerations were necessary to define the divested asset because Frontier divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. (Matt Pilon, "Frontier Unloads Northwest Telecom Assets for \$1.35B," HBJ, May 29, 2019, <https://www.hartfordbusiness.com/article/frontier-unloads-northwest-telecom-assets-for-135b>.) The public record that I have reviewed indicates that Frontier did not acquire the divested asset within ten years before the evaluated divestiture. Although Frontier acquired Verizon's wireline operations in Washington, Oregon, and Idaho in the 14-State Divestiture in 2010, the asset divested in 2019 was different than those acquired in 2010. First, the divested asset included Frontier's wireline operations in Montana, which it did not acquire from Verizon. (*See* "California, Nevada and South Carolina Approve Frontier Acquisition of Verizon Local Wireline Operations," Verizon News Archives, October 29, 2009, <https://www.verizon.com/about/news/press-releases/california-nevada-and-south-carolina-approve-frontier-acquisition-verizon-local-wireline-operations>). Second, the divested asset included the lines that Frontier operated in Oregon and Idaho prior to the 2010 14-State Divestiture, which were subsequently integrated with the operations purchased from Verizon. (*See* "Frontier Communications Announces Sale of Operations in Washington, Oregon, Idaho, and Montana," Frontier Communications, May 29, 2019, <https://investor.frontier.com/news/news-details/2019/Frontier-Communications-Announces-Sale-of-Operations-in-Washington-Oregon-Idaho-and-Montana-05-29-2019/default.aspx>; Citizens Communications Company, Form 10-K for the Fiscal Year Ended December 31, 2006, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/c1dd8f8d-65be-4a83-b357-0075cbe1fe54.pdf>, Exhibit 21.)

- c. CDK Global Inc.’s (“CDK”) 2021 sale of its international business, valued at \$1.45 billion, to Francisco Partners Management (“Francisco”);⁸¹ and
- d. Verizon’s 2016 sale of certain additional wireline operations, valued at \$10.54 billion, to Frontier.^{82,83}

45. The operational timelines alone of each of these four divestitures (701 days, 459 days, 432 days, and 398 days, respectively) took longer than the maximum of 360 days that the Act affords to Petitioners.⁸⁴ Moreover, consistent with the divested assets’ high level of pre-divestiture integration, each of these divestitures included a TSA or other forms of technological support services following deal close. As I described above, TSAs and similar technological

⁸¹ In CDK’s case, geographic considerations were necessary to define the divested asset because CDK divested its business in EMEA and Asia while retaining operations for the same products in other geographies. (*See* “Francisco Partners to Acquire International Business of CDK Global for \$1.45 Billion,” Francisco Partners, November 30, 2020, <https://www.franciscopartners.com/media/francisco-partners-to-acquire-international-business-of-cdk-global-for-145-billion>.) The public record that I have reviewed indicates that CDK did not acquire the divested asset within ten years before the evaluated divestiture. Although ADP spun off CDK in 2014, this spin-off is irrelevant when evaluating CDK’s 2021 divestiture of its international business. This is because, in 2021, CDK sold only one division of CDK (*i.e.*, its international business), rather than the entire entity that was spun off in 2014. Therefore, in 2021, CDK had to disentangle its international business from the rest of the entity. For this reason, the divested asset (*i.e.*, the international business) was not an asset that was acquired within 10 years of the announcement date. (*See* John Kirwan, “International Business of CDK Global Becomes Keyloop,” MotorTrader.com, March 1, 2021, <https://www.motortrader.com/motor-trader-news/automotive-news/307888-01-03-2021>.)

⁸² In Verizon’s case, geographic considerations were necessary to define the divested asset because Verizon divested its operations in some states while retaining the same operations (*i.e.*, same products supported by common systems) in some other states. The public record that I have reviewed indicates that Verizon did not acquire the divested asset within ten years before the evaluated divestiture. *See* “Frontier Communications Completes Acquisition of Verizon Wireline Operations in California, Texas and Florida,” April 1, 2016, <https://investor.frontier.com/news/news-details/2016/Frontier-Communications-Completes-Acquisition-of-Verizon-Wireline-Operations-in-California-Texas-and-Florida-04-01-2016/default.aspx>.

⁸³ Because this Verizon divestiture took place after I left Verizon, I do not have personal experience with this transaction. For this reason, I describe this divestiture in **Section III.D.2** instead of **Section III.D.1** (where I discussed other Verizon divestitures with which I am personally familiar).

⁸⁴ The corporate timeline alone of these divestitures (427, 339, 92, and 422 days, respectively) were similarly lengthy. However, as I described in **Section III.A**, I do not consider corporate timelines in my analysis because I have taken the conservative assumption in my declaration that TikTok would be able to achieve a corporate timeline of zero days.

support service agreements are not ideal for the seller or the buyer; therefore, the parties had an incentive to keep the observed operational timelines as short as possible.

- a. Lumen provided transition services to Apollo for “an average of 17 months [with the] right to extend the term of certain services for up to six months,” or up to 701 days.⁸⁵
- b. Frontier agreed to provide “various network and support services”⁸⁶ as well as “limited training and subject matter support services”⁸⁷ on July 31, 2019, and provided these services until October 31, 2020, or approximately 459 days.⁸⁸
- c. CDK entered a TSA with Fransico in November 2020 to assist in the integration of the international business.⁸⁹ CDK provided these services to Fransico until February 2022, for approximately 432 days.⁹⁰

⁸⁵ “Under the TSA, Lumen actually began providing transition services upon the October 3, 2022, completion date of the Divestiture. [...] The term of services to be provided under the TSA is an average of 17 months, subject to Apollo’s right to extend the term of certain services for up to six months and to terminate early the term of any service.” See Lumen Technologies, Inc., Form 8-K, dated October 3, 2022, <http://pdf.secdatabase.com/1788/0001193125-22-256669.pdf>.

⁸⁶ Frontier Communications, Form 10-K for the Fiscal Year Ended December 31, 2019, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/b7334365-f330-4e9d-8f5b-850623fd18d8.pdf>, p. 2.

⁸⁷ Frontier Communications, Form 10-K for the Fiscal Year Ended December 31, 2020, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/6b950dad-b24b-4079-ae7e-b089a4f71e59.pdf>, F-29.

⁸⁸ Frontier committed to planning the transition of operations at least as early as July 31, 2019. Testimony of Steve Weed, No. UT-190574, July 31, 2019, p. 37 (“Frontier has agreed to replicate its current IT systems”). Frontier stated that it stopped providing the services regulated by the TSA as of October 31, 2020.

⁸⁹ The TSA is attached to the Share Sale and Purchase Agreement dated November 27, 2020. Share Sale and Purchase Agreement by and Among CDK Global Holdings Ltd., the Other Restricted Entities Party Hereto, and Concorde Bidco Ltd., dated November 27, 2020, https://www.sec.gov/Archives/edgar/data/1609702/000160970221000005/cdk_q2fy21concorde-sharesa.htm.

⁹⁰ CDK Global, Inc., Form 10-Q for the Quarterly Period Ended March 31, 2022, p. 10. As the precise end date is unknown, I conservatively assumed that CDK’s transition services ended on February 1, 2022.

- d. Verizon entered a support agreement with Frontier in February 2015,⁹¹ and the transaction closed on April 1, 2016,⁹² *i.e.*, 398 days later.⁹³

46. These examples provide further evidence that divestitures of highly integrated assets: (1) consistently take more than 360 days; and (2) often necessitate post-closing services provided by the seller to the buyer to ensure business continuity. I note that—while these divestitures shared two indicia of complexity with the divestiture required of Petitioners (*i.e.*, a geographically defined divestiture of organically developed assets or assets held over ten years)—as I described in **Section III.C**, there are additional indicia of complexity associated with divesting TikTok’s U.S. application.

47. Additionally, **Exhibit 1** shows that, even when a divestiture involves assets that appear to be less integrated than TikTok’s U.S. application, the operational timelines for divestitures in the software industry (and in other industries within the TMT sector) nevertheless often take over 360 days.

⁹¹ The support agreement provided that the parties would develop a “joint Cutover Plan to set forth the processes, procedures, and steps through which the parties would prepare for and effect the cutover [*i.e.*, the switch from Verizon to Frontier following deal closing].” The parties “spent months” developing a 300-page plan (which created approximately 140 functional working teams, including teams from Engineering and IT). Response of Frontier California Inc. (U 1002 C) to Assigned Commissioner’s Ruling Inviting Party and Public Comments Regarding Issues Raised at Public Participation Hearings and Workshops in the Intrastate Rural Call Completion Issues Proceeding (I.14-05-012), September 20, 2016, <https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M168/K257/168257703.PDF>, Attachment A.

⁹² Frontier CPED Settlement Agreement, December 19, 2019, <https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M472/K024/472024199.pdf>, p. 2 (“[T]he transaction closed on April 1, 2016, and Frontier implemented a ‘cutover plan’ to transition the Verizon customers to Frontier’s service platform”).

⁹³ I conservatively assumed the start of the operational timeline March 1, 2015, *i.e.*, the first day after the cutover plan support agreement was entered. I considered the end of the operational timeline, April 1, 2016, the transaction close date. The resulting 398 days are consistent with a 2019 settlement agreement stating that “Frontier had been planning the transition for more than a year[.]” Frontier CPED Settlement Agreement, December 19, 2019, <https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M472/K024/472024199.pdf>, p. 2.

48. The 22 transactions remaining in my market sample all have indicia of less integration—and hence less complexity—than the four divestitures described above (as well as the three divestitures from Verizon that I personally experienced). In other words, each of the 22 remaining transactions involved either: (1) a divested asset defined solely by product market, or (2) the divestiture of an asset acquired within ten years of divestiture, or (3) both of these conditions.⁹⁴ Nevertheless, for these divestitures that have the indicia of less complexity than TikTok, the range of operational timelines often extended beyond 360 days.

49. For example, in the following eight divestitures, the divested asset was defined based solely on product market (*i.e.*, they have one of the indicia of a less complex divestiture than the divestiture required of Petitioners), and yet their expected or observable operational timelines were longer than 360 days:⁹⁵

⁹⁴ As shown in **Exhibit 1** and below, my market sample included no divestitures where the seller acquired the divested asset within ten years *and* the divested asset was defined solely by product market.

⁹⁵ For some divestitures in my market sample, I found information indicating the *de facto* operational timeline (*e.g.*, the beginning of planning activities as the observable start date, and the end of assistance provided by the seller as the observable end date of the operational timeline). For other divestitures in my sample, I found information only regarding the *de jure* operational timeline (*e.g.*, TSAs or similar documents including the time the parties expected it would take for the seller to provide transition services, *i.e.*, the *expected* operational timeline), without the *de facto* end date of the operational timeline. For this reason, I describe the operational timelines here as “expected or observable.” Given that—based on my experience and the literature (described above)—operational timelines are frequently underestimated, relying on the expected time presented in the TSA is likely a conservative estimate of the *de facto* operational timeline. For the same reason, where the available information provided a range as the expected operational timeline, I rely on the upper end of the range (while presenting the full range in **Exhibit 1**). *See, e.g.*, Yetton 2023, at p. 962 (“IT carve-out projects are notoriously problematic. IT carve-out projects frequently overrun timelines and budgets [...]. In part, this is because IT carve-out projects are frequently under-planned and underestimated”).

- a. Thomson Reuters Corporation's 2016 divestiture of its intellectual property and science business, valued at \$3.55 billion,⁹⁶ to Onex Corporation (operational timeline of 1,087 days).⁹⁷
- b. IAC Holdings, Inc.'s 2020 spin-off of Match Group, Inc., valued at \$8.09 billion⁹⁸ (operational timeline of 732 days);⁹⁹

⁹⁶ See "Thomson Reuters Announces Definitive Agreement to Sell Its Intellectual Property & Science Business to Onex and Baring Asia for \$3.55 Billion," PR Newswire, July 11, 2016, <https://www.prnewswire.com/news-releases/thomson-reuters-announces-definitive-agreement-to-sell-its-intellectual-property--science-business-to-onex-and-baring-asia-for-355-billion-300296352.html>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

⁹⁷ I considered the start of the operational timeline the date of the TSA, July 10, 2016. I conservatively assumed the end of the operational timeline to be July 1, 2019, because the buyer recorded "payments to Thomson Reuters under the [TSA]" during the three months ended on September 30, 2019. See "Clarivate Analytics Reports Third Quarter 2019 Results," Clarivate Analytics, November 6, 2019, <https://clarivate.com/news/clarivate-analytics-reports-third-quarter-2019-results/>.

⁹⁸ See "IAC and Match Group Complete Full Separation," IAC, July 1, 2020, <https://www.iac.com/press-releases/iac-and-match-group-complete-full-separation>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. Match.com was acquired by TMCS (Ticketmaster Online-CitySearch Inc.) in June 1999 (*i.e.*, more than ten years before this divestiture's announcement date). In 2003 (still more than ten years before this divestiture's announcement date), IAC acquired TMCS, and following Match.com's IPO on November 24, 2014, IAC retained a significant stake in the company. See "25 Year Innovator," IAC, <https://www.iac.com/history>; "IAC and Match Group Announce Closing of Initial Public Offering," IAC, November 24, 2015, <https://www.iac.com/press-releases/iac-and-match-group-announce-closing-of-initial-public-offering>.

⁹⁹ I considered the start of the operational timeline the date of the TSA, June 30, 2020. (See IAC/InterActiveCorp and IAC Holdings, Inc., Transition Services Agreement by and Between IAC/InterActiveCorp and IAC Holdings, Inc., dated June 30, 2020, https://www.sec.gov/Archives/edgar/data/1800227/000110465920080610/tm2022502d7_ex10-1.htm.) I conservatively assumed the end of the operational timeline to be July 1, 2022, because the seller recorded revenues "from IAC for services provided to IAC under the transition services agreement" during the three-month period ended September 30, 2022. Match Group, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2022, dated November 4, 2022, <https://www.sec.gov/Archives/edgar/data/891103/000089110322000095/match-20220930.htm>, p. 27.

- c. IAC Inc.'s 2021 spin-off of Vimeo, Inc., valued at \$7.68 billion¹⁰⁰ (operational timeline of at least 588 days);¹⁰¹
- d. SolarWinds Corporation's 2021 spin-off of its Managed Service Provider (MSP) business into N-able, Inc., valued at \$2.05 billion¹⁰² (expected operational timeline of 534 days);¹⁰³

¹⁰⁰ See "IAC Completes Spin-Off Of Vimeo," IAC, May 25, 2021, <https://www.iac.com/press-releases/iac-completes-spin-off-of-vimeo>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹⁰¹ I considered the start of the operational timeline the date of the TSA, May 24, 2021. I made the conservative assumption that the end of the operational timeline is January 1, 2023, because, as of at least January 1, 2023, IAC continued to receive fees "for services rendered pursuant to the transition services agreement." See IAC/InterActiveCorp and Vimeo, Inc., Transition Services Agreement by and Between IAC/InterActiveCorp and Vimeo, Inc., dated May 24, 2021, https://www.sec.gov/Archives/edgar/data/1837686/000110465921073207/tm2117737d1_ex10-3.htm; IAC/InterActiveCorp and Vimeo, Inc., Extension Request #2 Pursuant to Transition Services Agreement by and Between IAC/InterActiveCorp and Vimeo, Inc., dated June 30, 2022, <https://www.sec.gov/Archives/edgar/data/1837686/000183768622000022/ex101-2022630.htm>; IAC Inc., Form 10-Q for the Quarterly Period Ended March 31, 2023, <https://www.sec.gov/Archives/edgar/data/1800227/000180022723000016/iaci-20230331.htm>.

¹⁰² See "SolarWinds Completes Spin-Off of its MSP Business; N-able, Inc. Begins Trading as Independent, Publicly Traded Company," SolarWinds, July 20, 2021, <https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Completes-Spin-Off-of-its-MSP-Business-N-able-Inc.-Begins-Trading-as-Independent-Publicly-Traded-Company/default.aspx>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. I note that SolarWinds' 2013 acquisition of a *different* company that was also called "N-able" is irrelevant for this evaluation. Following this 2013 acquisition, SolarWinds integrated the assets of N-able with the assets of another company that SolarWinds acquired in 2016 (LOGICnow) to create "SolarWindsMSP." Then, in 2021, SolarWinds spun off "SolarWindsMSP" as a new entity, which SolarWinds named "N-able." See Stefanie Hammond, "Happy anniversary to me!," N-able, November 24, 2021, <https://www.n-able.com/fr/blog/happy-anniversary-to-me>.

¹⁰³ The TSA was dated as of July 16, 2021, and the transition services were expected to end on December 31, 2022. See Transition Services Agreement by and Between SolarWinds Corporation and N-Able, Inc., dated July 16, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000162828021014064/exhibit101-swinxable8xk.htm>. See also SolarWinds Corporation, Form 10-K for the Fiscal Year Ended December 31, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000173994222000020/swi-20211231.htm>, p. F-36 ("The transition services agreement will terminate on the expiration of the term of the last service provided under it, which SolarWinds anticipates to be on or around December 31, 2022.").

- e. Micro Focus International plc's 2017 acquisition of Hewlett Packard's software business, valued at \$9.00 billion¹⁰⁴ (expected operational timeline of up to 456 days);¹⁰⁵
- f. Automatic Data Processing, Inc.'s 2014 spin-off of its automotive dealer services product business, valued at \$4.94 billion¹⁰⁶ (operational timeline of at least 367 days);¹⁰⁷

¹⁰⁴ "UK Tech Giant Micro Focus Plunges in Value as Shares Crash," BBC, March 19, 2018, <https://www.bbc.com/news/business-43457024> (Micro Focus International plc "purchase[d] [...] Hewlett Packard Enterprise's software business for £6.8bn."). I used the U.S. dollar value of \$9.00 billion as reported by S&P Capital IQ Pro. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹⁰⁵ See Transition Services Agreement by and Between Hewlett Packard Enterprise Company and Seattle SpinCo, Inc., dated September 1, 2017, https://www.sec.gov/Archives/edgar/data/1645590/000156761917001826/s001851x1_ex2-3.htm; Seattle SpinCo, Inc. and Micro Focus International plc, Form 424B3, dated August 15, 2017, https://www.sec.gov/Archives/edgar/data/1359711/000156761917001747/s001838x1_424b3.html 149, p. 219 ("The initial term of the Transition Services Agreement will be nine months, and each party in certain circumstances may extend the term of services it will receive for up to two three-month periods (for a total term of up to 15 months)").

¹⁰⁶ See "ADP Completes Spin-Off of Automotive Dealer Services Business," Paul Weiss, September 30, 2014, <https://www.paulweiss.com/practices/transactional/corporate/news/adp-completes-spin-off-of-automotive-dealer-services-business?id=18827> ("Automatic Data Processing, Inc. (ADP) completed the distribution to its stockholders of all of the issued and outstanding common stock of CDK Global, Inc. in a tax-free spin-off. The distribution completes the spin-off by ADP of its automotive dealer services business"). The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹⁰⁷ I considered the start of the operational timeline the date of the TSA, September 29, 2014. I considered the end of the operational timeline September 30, 2015, the last date of the transitional period "pursuant to the transition services agreement" with ADP. See CDK Global, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2014, https://www.sec.gov/Archives/edgar/data/1609702/000160970214000006/cdk_q1fy1510-q.htm, p. 34; CDK Global, Inc., Form 10-Q for the Quarterly Period Ended December 31, 2015, https://www.sec.gov/Archives/edgar/data/1609702/000160970216000037/cdk_q2fy1610-q.htm, p. 7.

- g. Symantec Corporation's 2017 divestiture of its website security business, valued at \$1.12 billion,¹⁰⁸ to DigiCert, Inc. (operational timeline of at least 365),¹⁰⁹ and
 - h. IBM Corporation's 2019 divestiture of its software portfolio of international business, valued at \$1.78 billion,¹¹⁰ to HCL Technologies Ltd. (expected operational timeline up to over 365 days).¹¹¹
50. Similarly, in the following five divestitures, the divested asset was defined based solely on product market *and* the seller acquired the divested asset within ten years before the divestiture (*i.e.*, they have both indicia of a less complex divestiture than the one required of

¹⁰⁸ See John Merrill, "DigiCert to Acquire Symantec's Website Security Business," DigiCert, August 2, 2017, <https://www.digicert.com/blog/digicert-to-acquire-symantec-website-security-business>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹⁰⁹ See Purchase Agreement by and Among Symantec Corporation, DigiCert Parent, Inc., and DigiCert, Inc., dated August 2, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939917000016/a092917exhibit21.htm>, pp. 111-112 ("Unless otherwise agreed by Arion (refers to DigiCert) and Sphinx (refers to Symantec) or set forth in the Preliminary Transition Service Schedules, no Transition Period will last for more than 12 months following the Closing Date (excluding any extensions made to the Transition Period in accordance with the terms of the Transition Services Agreement)"). See also Symantec Corporation, Form 10-Q for the Quarterly Period Ended December 29, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939918000004/symc122917-10q.htm>, p. 14 ("The services under the TSA commenced with the close of the transaction and expire at various dates through fiscal 2019, with extension options").

¹¹⁰ See "HCL Technologies to Buy IBM Software Products in \$1.8 Billion Deal," Nikkei Asia, December 7, 2018, <https://asia.nikkei.com/Business/Companies/HCL-Technologies-to-buy-IBM-software-products-in-1.8-billion-deal>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹¹¹ For the lower bound of the operational timeline, I conservatively assumed that the start date is January 31, 2019, because HCL Tech announced in January 2019 that "HCL is working on a smooth transition plan." As the end date, I conservatively used the date of the deal close, June 30, 2019. For the upper bound, I conservatively used 365 days because IBM stated that "HCL can renew certain [transition] services up to an additional year." See "HCL Announces Acquisition of Select IBM Products Frequently Asked Questions," Products & Platforms, https://www.hcltech.com/sites/default/files/documents/inline-migration/general_faq_jan_2019.pdf, p. 3; IBM Corporation, Form 10-Q for the Quarter Ended September 30, 2019, <https://www.sec.gov/Archives/edgar/data/51143/000155837019009324/ibm-20190930x10q.htm>, p. 52.

Petitioners), and yet they too have expected or observable operational timelines longer than 360 days:

- a. Xperi Holding Corporation's 2022 spin-off of its product business from its intellectual property licensing business, valued at \$1.08 billion¹¹² (operational timeline of at least 844 days);¹¹³
- b. TEGNA Inc.'s 2017 spin-off of Cars.com Inc., valued at \$1.85 billion¹¹⁴ (operational timeline of up to 24 months, *i.e.*, 730 days);¹¹⁵

¹¹² Xperi (formerly Tessera Holding Corporation) acquired the product business of DTS, Inc in December 2016, *i.e.*, six years before this divestiture. (See "Tessera Completes Acquisition of DTS," Business Wire, December 1, 2016, <https://www.businesswire.com/news/home/20161201005268/en/Tessera>; "Tessera Holding Corporation Announces Name Change to Xperi Corporation," Xperi, February 22, 2017, <https://investor.xperi.com/news/news-details/2017/Tessera-Holding-Corporation-Announces-Name-Change-to-Xperi-Corporation/default.aspx>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

¹¹³ While I have found neither the precise start date nor the precise end date of the operational timeline from public documents, I was able to estimate the operational timeline by using conservative proxy dates for both. As the start date, I used July 1, 2020, which is the first day following the month in which Xperi publicly announced its intention to divest its assets (June 2020). Using this date as the start of the operational timeline is conservative because public announcements typically occur following internal operational planning. As the end date, I used October 22, 2022, the date of the first amendment to the TSA. This date is conservative as the implementation of the TSA is likely to continue after its amendment date. See Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2023, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001788999/0768588f-717f-4908-a897-745524c9f289.pdf>, pp. 51-52; Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2022, <https://www.sec.gov/ix?doc=/Archives/edgar/data/1788999/000095017023006053/xper-20221231.htm>, p. 105.

¹¹⁴ See "Cars.com Completes Spin-off from Parent Company TEGNA," Cars.com, June 1, 2017, <https://www.cars.com/articles/carscom-completes-spin-off-from-parent-company-tegna-1420695567172/>. Gannett, the corporate predecessor of TEGNA, acquired Cars.com in 2014, *i.e.*, three years before this divestiture. (See Veronica Garabelli, "Gannett Acquires Cars.com for \$1.8 Billion," Virginia Business, October 1, 2014, <https://www.virginiabusiness.com/article/gannett-acquires-cars-com-for-1-8-billion/>; "Separation of Gannett into Two Public Companies Completed," TEGNA, June 29, 2015, <https://www.tegna.com/separation-of-gannett-into-two-public-companies-completed/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

¹¹⁵ TEGNA and Cars.com entered a TSA on May 31, 2017, pursuant to which TEGNA agreed to "provide certain services to Cars.com on an interim and transitional basis, not to exceed 24 months." See Transition Services Agreement by and Between TEGNA Inc. and Cars.com Inc., dated May 31, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000119312517196074/d514170dex101.htm>; TEGNA Inc., Form 10-Q for the Quarterly Period Ended September 30, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000003989917000041/tgna-20170930x10q.htm>, p.20.

- c. FireEye, Inc.’s 2021 divestiture of its products business, valued at \$1.2 billion,¹¹⁶ to Symphony Technology Group (expected operational timeline of up to 548 days);¹¹⁷
- d. Dell Technologies Inc.’s 2021 spin-off of VMware LLC, valued at \$51.14 billion¹¹⁸ (expected operational timeline of up to 365 days);¹¹⁹

¹¹⁶ See “FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion,” Mandiant, June 2, 2021, <https://www.mandiant.com/company/press-releases/fireeye-announces-sale-fireeye-products-business-symphony-technology-group>. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. See Zacks Equity Research, “FireEye Rebrands as Mandiant (FEYE) After Product Biz Sell-Off,” Nasdaq, October 5, 2021, <https://www.nasdaq.com/articles/fireeye-rebrands-as-mandiant-feye-after-product-biz-sell-off-2021-10-05> (“Through this transaction, [FireEye] undoes its 2014 acquisition, which brought Mandiant solutions and FireEye products together”).

¹¹⁷ On June 2, 2021, FireEye said it would enter a TSA at closing. See FireEye, Symphony Technology Group, FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion, https://www.sec.gov/Archives/edgar/data/1370880/000110465921075725/tm2118082d1_ex99-1.htm (“[FireEye] at closing will enter into agreements [which] include [...] a transition services agreement”); FireEye, Inc., Form 10-Q for the Quarterly Period Ended June 30, 2021, <https://www.sec.gov/Archives/edgar/data/1370880/000137088021000033/feye-20210630.htm>, p. 12 (“The transition period is expected to be approximately 12 to 18 months after the sale closes”).

¹¹⁸ See “Dell Technologies Announces Completion of VMware Spin-off,” Dell Technologies, November 1, 2021, <https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2021~11~20211101-dell-technologies-announces-completion-of-vmware-spin-off.htm#/filter-on/Country:en-us>. Dell acquired VMware in 2015, *i.e.*, six years before this divestiture. (See Ron Miller and Alex Wilhelm, “Dell Is Spinning Out VMware in a Deal Expected to Generate Over \$9B for the Company,” TechCrunch, April 14, 2021, <https://techcrunch.com/2021/04/14/dell-is-spinning-out-vmware-in-a-deal-expected-to-generate-over-9b-for-the-company/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

¹¹⁹ See Dell Technologies Inc., Form 8-K, dated October 29, 2021, <https://investors.delltechnologies.com/static-files/072b94f3-090e-4891-a825-0014a787b6c9>, p. 4 (“In connection with the Spin-Off, on November 1, 2021, Dell entered into a [...] Transition Services Agreement[.]”). See also Dell Technologies Inc., Form 10-Q for the Quarterly Period Ended October 28, 2022, <https://www.sec.gov/Archives/edgar/data/1571996/000157199622000044/dell-20221028.htm>, pp. 15, 49 (“Transition services may be provided for up to one year”).

- e. Dell EMC's 2017 divestiture of its Enterprise Content Division, valued at \$1.62 billion,¹²⁰ to Open Text Corporation (expected operational timeline up to over 365 days).¹²¹

51. These examples illustrate that the divestiture of integrated assets often take over 360 days even when the level of integration is expected to be relatively low, as evidenced by a divested asset that can be defined based solely on product market and/or the divestiture of a recently-acquired asset. While these examples would not be representative of the high level of integration that exists between TikTok's U.S. application and its global application (or ByteDance), they nevertheless show that divestitures are complex and time-consuming processes, which often require post-closing services from the seller to ensure business continuity. Again, these types of services would not be possible under a "qualified divestiture."

52. To be sure, when the level of integration and complexity is lower than what exists with respect to TikTok's U.S. application and its global application (or ByteDance), the operational timeline of divestitures can take fewer than 360 days. However, based on the divestitures in my sample for which I was able to identify an operational timeline, these still take well over 270 days. In case of all three divestitures below, the divested asset was defined based

¹²⁰ See "OpenText Signs Definitive Agreement to Acquire Dell EMC's Enterprise Content Division, including Documentum," PR Newswire, September 12, 2016, <https://www.prnewswire.com/news-releases/opentext-signs-definitive-agreement-to-acquire-dell-emcs-enterprise-content-division-including-documentum-300326059.html>. Dell acquired EMC in 2016, *i.e.*, the year of this divestiture. (See Noreen Seebacher, "OpenText Acquires Dell EMC's Enterprise Content Division, Including Documentum," CMSWire, September 12, 2016, <https://www.cmswire.com/information-management/opentext-acquires-dell-emcs-enterprise-content-division-including-documentum/>.) The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset.

¹²¹ See Dell Technologies Inc., Form 10-K for the Fiscal Year Ended February 2, 2018, <https://investors.delltechnologies.com/static-files/9d4aca86-7fd6-4b4f-ab4b-4895fa562826>, p. 104 ("Transition services may be provided for up to one year, with an option to renew after that period").

solely on product market (*i.e.*, they have one of the indicia of a less complex divestiture than the divestiture required of Petitioners),¹²² and they still took well over 270 days. Specifically:

- a. The operational timeline of Citrix Systems Inc.'s 2017 divestiture of its GoTo subsidiary, valued at \$2.85 billion, to LogMeIn Inc. took 335 days.¹²³
- b. The operational timeline of Symantec's 2019 divestiture of its enterprise security business, valued at \$10.70 billion, to Broadcom took 330 days.¹²⁴
- c. The operational timeline of Altaba Inc.'s 2017 divestiture of Yahoo!'s operating business, valued at \$4.48 billion, to Verizon took 324 days.¹²⁵

¹²² See Liana B. Baker, "LogMeIn to Merge with Citrix's GoTo Unit in All-Stock Deal," Yahoo Finance, July 26, 2016, <https://finance.yahoo.com/news/logmein-merge-citrixs-goto-unit-002645133.html>; "Broadcom to Acquire Symantec Enterprise Security Business for \$10.7 Billion in Cash," Broadcom, August 8, 2019, <https://investors.broadcom.com/news-releases/news-release-details/broadcom-acquire-symantec-enterprise-security-business-107>; "Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary," Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsidiary>. For all three of these divestitures, the public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

¹²³ I considered the start of the operational timeline the date of the TSA, January 31, 2017. I considered the end of the operational timeline December 31, 2017, the date when the company stated that "the transition services are substantially complete." See LogMeIn, Inc., Form 10-K for the Fiscal Year Ended December 31, 2016, <https://www.sec.gov/Archives/edgar/data/1420302/000119312517063977/d301311d10k.htm#toc>, p. 90; LogMeIn, Inc., Form 10-K for the Fiscal Year Ended December 31, 2017, <https://www.sec.gov/Archives/edgar/data/1420302/000119312518050503/d506130d10k.htm>, p. 71.

¹²⁴ I considered the start of the operational timeline August 8, 2019, the date of the Asset Purchase Agreement to which the TSA was attached. I conservatively considered the end of the operational timeline July 2, 2020, because the parties reported having incurred transition services costs "during the three [...] months ended October 2, 2020." See Asset Purchase Agreement by and Between Broadcom Inc. and Symantec Corporation, dated August 8, 2019, <https://www.sec.gov/Archives/edgar/data/1730168/000119312519217369/d790567dex21.htm>; NortonLifeLock Inc., Form 10-Q for the Quarterly Period Ended October 2, 2020, <https://www.sec.gov/Archives/edgar/data/849399/000084939920000011/nlok-20201002.htm>, p. 10.

¹²⁵ I conservatively considered the start of the operational timeline July 25, 2016, because "the Yahoo transaction was announced" in July 2016. I considered the end of the operational timeline June 13, 2017, the date when "Oath beg[an] operation[.]" See "Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary," Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsidiary> (Oath CEO "has been leading integration planning teams since the Yahoo transaction was announced in July 2016").

53. In other words, from the 26 divestitures that satisfied the criteria described in paragraphs 42-43,¹²⁶ and for which I could identify the beginning and end of the operational timeline, I have found none where the operational timeline took fewer than 270 days (in fact, I have found none with an operational timeline shorter than 324 days).^{127,128} **Figure 2** below summarizes the results of my analysis based on: (i) the three Verizon divestitures described in **Section III.D.1**, and (ii) the 26 divestitures in my market sample.

¹²⁶ *I.e.*, divestiture transactions where: (1) the divested assets operated in the following industries: “interactive media and services,” “application software,” “systems software,” or “integrated telecommunication services;” (2) the transaction (i) took place in the United States, (ii) was announced and completed in the last ten years (between 2014 and 2024), and (iii) had a total transaction value greater than \$1 billion; and (3) at least one of the buyer or the seller had publicly available SEC filings at the time of the divestiture, and the transaction was subject to regulatory or antitrust approval.

¹²⁷ In the case of the six remaining divestitures from this sample, I was unable to identify an operational timeline because I could not find a start date, end date, or both. All six of these divestitures have indicia of less complexity than the divestiture required of Petitioners (*i.e.*, the divested asset was defined based solely on product market and/or the seller acquired the divested asset within ten years before the divestiture). These are: (1) XO Holdings, Inc.’s 2017 divestiture of its fiber-optics network business to Verizon, (2) Bain Capital, LP’s and other entities’ 2016 divestiture of the mobile and web assets of Weather Channel LLC to IBM Corporation, (3) LiveRamp Holdings, Inc.’s 2018 divestiture of its Acxiom marketing solutions business to The Interpublic Group of Companies Inc. (4) Lumen Technologies, Inc.’s 2017 divestiture of its data centers and colocation business to BC Partners and other entities, (5) Intrado Corporation’s and Apollo Global Management, Inc.’s 2023 divestiture of its safety business to Stonepeak Partners LP, and (6) Aon plc’s 2017 sale of its “technology-enabled benefits and human resources platform” to Tempo Acquisition, LLC, Blackstone Group L.P. *See Exhibit 1.*

¹²⁸ As I described in footnote 17, from the day of submitting my declaration on June 20, 2024, Petitioners have only 214 days left until January 19, 2025; and they have only 304 days left until April 19, 2025.

**Figure 2 - Number of Divestitures in the TMT Sector,
Grouped by Indicia of Complexity and Length of Operational Timeline¹²⁹**

Operational timeline	Highly integrated based on both indicia	Less integrated based on at least one indicia	Total
Over 360 days	7	13	20
Under 360 days but over 270 days	0	3	3
Under 270 days	0	0	0
Unknown length	0	6	6
Total	7	22	29

54. This analysis is consistent with information provided by Petitioners to CFIUS, which estimates that migrating TikTok’s software, including its recommendation engine and internal tools, would take at least approximately two years.¹³⁰ Critically, this two-year timeline was premised on several significant operational assumptions and caveats. For instance, the timeline assumes that not all tools and processes would be migrated; for example, “Content Moderation Systems will continue to be developed in China but be subject to open source to the public,”¹³¹ and there would be continued access to “internal reference code from global development.”¹³² Additionally, this two-year timeline relates to migrating certain tools to “TikTok employees working in locations where the TikTok service is offered.”¹³³ So, even if the

¹²⁹ As described in footnote 95, given that operational timelines are frequently underestimated, where the available information provided a range as the expected operational timeline, I present in this table the upper end of the range (while presenting the full range in **Exhibit 1**).

¹³⁰ NSA Presentation, 2023, p. 16.

¹³¹ NSA Presentation, 2023, p. 16.

¹³² NSA Presentation, 2023, p. 13.

¹³³ NSA Presentation, 2023, p. 13.

two-year timeline were met, it would not sever all “operational relationships” between Petitioners and TikTok’s U.S. application.

55. Finally, I note that—although a member of Congress suggested that Kunlun’s (a Chinese video game company’s) 2020 divestiture of the Grindr application indicates that Petitioners will be able to divest TikTok’s U.S. application “quickly” and with “no disruption to users”¹³⁴—there are several reasons why this comparator is incorrect. Unlike the high level of integration between TikTok’s U.S. application and its global application (or ByteDance), Grindr was not highly integrated with Kunlun before its divestiture. Therefore, the Grindr divestiture did not require untangling highly integrated assets.

- a. First, Grindr was developed as a separate business from Kunlun, and Kunlun acquired a majority share in Grindr only four years before the divestiture.¹³⁵
- b. Second, the divestiture did not involve the untangling of assets within the Grindr platform, as Kunlun acquired and then divested Grindr in its entirety—in other words, Kunlun simply unwound the acquisition from four years prior.¹³⁶

Accordingly, S&P Capital IQ Pro categorizes the Grindr divestiture as “M&A –

¹³⁴ “[TikTok’s] divestment requirement is not new. It is not without precedent. When the app Grindr [...] was acquired by a Chinese company [...] the U.S. Government [...] required divestment. This happened quickly. Why? Because Grindr was a very valuable social media company. The same is true with regard to TikTok. There will be no disruption to users, just as there was [no disruption] with Grindr.” See “House Debate on H.R. 7521, H1163-1171,” Congressional Record — House, March 13, 2024, <https://www.congress.gov/118/crec/2024/03/13/170/45/CREC-2024-03-13-pt1-PgH1163-2.pdf> (Rep. Krishnamoorthi, at H1165).

¹³⁵ See Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” Los Angeles Times, March 6, 2020, <https://web.archive.org/web/20200403002228/https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns>.

¹³⁶ See Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” Los Angeles Times, March 6, 2020, <https://web.archive.org/web/20200403002228/https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns>.

Whole,” indicating that this transaction involved the sale of a whole legal entity, rather than the divestiture of a subset of assets within the company that needed to be untangled and separated.¹³⁷

- c. Third, the fact that the Grindr divestiture did not require untangling highly integrated assets is also evidenced by Kunlun’s planned 2018 IPO of Grindr,¹³⁸ suggesting that Grindr was easily separable from the rest of Kunlun already as of 2018.
- d. Finally, even though Grindr was substantially less integrated with Kunlun than TikTok’s U.S. application and its global application (or ByteDance), CFIUS still provided Kunlun with more time to divest Grindr than what the Act affords to Petitioners. Specifically, the CFIUS NSA (signed on May 9, 2019) provided Kunlun with 419 days to divest.¹³⁹ In fact, Kunlun and the buyer did not sign an “Amended and Restated Stock Purchase Agreement” until May 13, 2020 (*i.e.*, 371 days after the execution of the NSA), showing that even this less complex divestiture was not completed within 360 days.

¹³⁷ This is the reason why the Grindr divestiture was not part of the 26 TMT divestitures I analyzed. As described in footnote 70, to identify divestiture transactions in S&P Capital IQ Pro, I used the filter “Transaction Type” to select transactions that were either “M&A - Asset” or “M&A - Spinoff or Splitoff.”

¹³⁸ See “Grindr: Chinese Parent Company Plans to List Gay Dating App,” BBC, July 30, 2019, <https://www.bbc.com/news/business-49160406>.

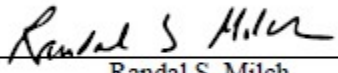
¹³⁹ The NSA was signed with CFIUS on May 9, 2019, and it ordered Kunlun to divest Grindr by June 30, 2020. See Trade Practitioner, “CFIUS Mitigation: Beijing Kunlun Wanwei Technology Co. and Grindr Inc.,” Squire Patton Boggs, June 19, 2019, <https://www.tradepractitioner.com/2019/06/cfius-beijing-kunlun-wanwei-technology-grindr/>.

E. A “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within the timeline required by the Act

56. As I showed in **Section III.C**, TikTok’s U.S. application is highly integrated with the global TikTok application (and with ByteDance). Additionally, as I showed in **Section III.D**, the operational timeline alone (*i.e.*, not considering the corporate timeline) of complex divestitures of highly integrated technical assets consistently takes over 360 days and necessitates post-closing support from the seller. Furthermore, the operational timeline of even less integrated assets also often takes over 360 days, and I have found no examples from the 26 divestitures in my market sample where the operational timeline took fewer than 270 days.

57. Therefore, the available information and my experience with complex divestitures support my opinion that a “qualified divestiture” of TikTok’s U.S. application is not operationally feasible within 360 days (let alone within 270 days).

Pursuant to 28 U.S.C § 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on June 17, 2024.



Randal S. Milch

Exhibit 1

Exhibit 1
Summary of Divestitures Reviewed

Divestiture						Extent of Integration		Observable Number of Days	
#	Divested Asset/Target ^[1]	Seller ^[1]	Buyer ^[1]	Total Transaction Value (\$M) ^[1]	Industry of Target ^[1]	Is the divested asset defined solely on product market (as opposed to geographic market)?	Did the seller acquire the divested asset within 10 years of the evaluated divestiture?	Observable Corporate Timeline (total days from (1) announcement date to (2) closing date) ^[1]	Observable / Expected Operational Timeline (total days from (1) evidence of planning the transition to (2) no more expected or actual assistance from the seller) ^[2]
A1	TikTok U.S. Application	ByteDance	Unknown	Unknown	Interactive Media and Services	No ³	No ⁴		
B1	Northeast Business	Verizon Communications Inc.	FairPoint Communications, Inc.	2,715	Integrated Telecommunication Services	No ⁵	No ⁶	442	727 ⁷
B2	14-State Divestiture	Verizon Communications Inc.	Frontier Communications Corporation	8,500	Integrated Telecommunication Services	No ⁸	No ⁹	415	642 ¹⁰
B3	HawaiianTel	Verizon Communications Inc.	The Carlyle Group	1,650	Integrated Telecommunication Services	No ¹¹	No ¹²	417	422 ¹³
C1	ILEC business of Lumen Technologies, Inc.	Lumen Technologies, Inc.	Apollo Global Management, Inc.	7,500	Integrated Telecommunication Services	No ¹⁴	No ¹⁵	427	517-701 ¹⁶
C2	Northwest operations and assets of Frontier Communications ¹⁷	Frontier Communications Parent, Inc.	British Columbia Investment Management Corporation; Public Sector Pension Investment Board; Canada Pension Plan Investment Board; Searchlight Capital Partners, L.P.; WaveDivision Capital LLC	1,352	Integrated Telecommunication Services	No ¹⁸	No ¹⁹	339	459 ²⁰
C3	International business segment of CDK Global, Inc.	CDK Global, Inc.	Francisco Partners Management, L.P.	1,450	Application Software	No ²¹	No ²²	92	432 ²³
C4	Verizon's wireline operations in California, Texas and Florida ²⁴	Verizon Communications Inc.	Frontier Communications Parent, Inc.	10,540	Integrated Telecommunication Services	No ²⁵	No ²⁶	422	398 ²⁷

Exhibit 1
Summary of Divestitures Reviewed

Divestiture						Extent of Integration		Observable Number of Days	
#	Divested Asset/Target ^[1]	Seller ^[1]	Buyer ^[1]	Total Transaction Value (\$M) ^[1]	Industry of Target ^[1]	Is the divested asset defined solely on product market (as opposed to geographic market)?	Did the seller acquire the divested asset within 10 years of the evaluated divestiture?	Observable Corporate Timeline (total days from (1) announcement date to (2) closing date) ^[1]	Observable / Expected Operational Timeline (total days from (1) evidence of planning the transition to (2) no more expected or actual assistance from the seller) ^[2]
C5	Intellectual Property & Science business of Thomson Reuters Corporation	Thomson Reuters Corporation	Onex Corporation; EQT Private Capital Asia	3,550	Application Software	Yes ²⁸	No ²⁸	85	1,087 ³⁰
C6	Match Group, Inc. ³¹	IAC Holdings, Inc. ³¹	Spinoff/Splitoff	8,086	Interactive Media and Services	Yes ³²	No ³³	264	732 ³⁴
C7	Vimeo, Inc.	IAC Inc.	Spinoff/Splitoff	7,679	Interactive Media and Services	Yes ³⁵	No ³⁶	154	588 ³⁷
C8	SolarWinds MSP ³⁸	SolarWinds Corporation	Spinoff/Splitoff	2,052	Systems Software	Yes ³⁹	No ⁴⁰	348	534 ⁴¹
C9	Software business of Hewlett Packard Enterprise	Hewlett Packard Enterprise	Micro Focus International plc	9,004	Application Software	Yes ⁴²	No ⁴³	360	273-456 ⁴⁴
C10	ADP Dealer Services, Inc.	Automatic Data Processing, Inc.	Spinoff/Splitoff	4,939	Application Software	Yes ⁴⁵	No ⁴⁶	174	367 ⁴⁷
C11	Website security business of Symantec Corporation	Symantec Corporation ⁴⁸	DigiCert, Inc.	1,119	Systems Software	Yes ⁴⁹	No ⁵⁰	91	up to over 365 ⁵¹
C12	Software portfolio of IBM Corp.	IBM Corporation	HCL Technologies Ltd.	1,775	Application Software	Yes ⁵²	No ⁵³	206	151-up to over 365 ⁵⁴
C13	GoTo subsidiary of Citrix Systems, Inc.	Citrix Systems, Inc.	LogMeIn Inc. ⁵⁵	2,848	Application Software	Yes ⁵⁶	No ⁵⁷	190	335 ⁵⁸
C14	Enterprise security business of Symantec Corporation	Symantec Corporation ⁵⁹	Broadcom Inc.	10,700	Systems Software	Yes ⁶⁰	No ⁶¹	89	330 ⁶²
C15	Yahoo's operating business	Altaba Inc.	Verizon Communications Inc.	4,476	Application Software	Yes ⁶³	No ⁶⁴	324	324 ⁶⁵
C16	Fiber-optic network business of XO Holdings, Inc.	XO Holdings, Inc.	Verizon Communications Inc.	1,800	Integrated Telecommunication Services	Yes ⁶⁶	No ⁶⁷	346	n/a

Exhibit 1
Summary of Divestitures Reviewed

Divestiture						Extent of Integration		Observable Number of Days	
#	Divested Asset/Target ^[1]	Seller ^[1]	Buyer ^[1]	Total Transaction Value (\$M) ^[1]	Industry of Target ^[1]	Is the divested asset defined solely on product market (as opposed to geographic market)?	Did the seller acquire the divested asset within 10 years of the evaluated divestiture?	Observable Corporate Timeline (total days from (1) announcement date to (2) closing date) ^[1]	Observable / Expected Operational Timeline (total days from (1) evidence of planning the transition to (2) no more expected or actual assistance from the seller) ^[2]
C17	Mobile and web assets of Weather Channel LLC	Bain Capital, LP; NBCUniversal Media, LLC; Blackstone Inc.	IBM Corporation	2,284	Application Software	Yes ⁶⁸	No ⁶⁹	94	n/a
C18	Axiom marketing solutions business	LiveRamp Holdings, Inc.	The Interpublic Group of Companies Inc.	2,300	Application Software	Yes ⁷⁰	No ⁷¹	92	n/a
C19	Xperi Inc.	Xperi Holding Corporation	Spinoff/Splitoff	1,084	Systems Software	Yes ⁷²	Yes ⁷³	61	844 ⁷⁴
C20	Cars.com Inc.	TEGNA Inc.	Spinoff/Splitoff	1,854	Interactive Media and Services	Yes ⁷⁵	Yes ⁷⁶	267	730 ⁷⁷
C21	Products business of FireEye, Inc.	FireEye, Inc. ⁷⁸	Symphony Technology Group ⁷⁹	1,200	Systems Software	Yes ⁸⁰	Yes ⁸¹	129	365-548 ⁸²
C22	VMware LLC	Dell Technologies Inc.	Spinoff/Splitoff	51,143	Systems Software	Yes ⁸³	Yes ⁸⁴	202	270-365 ⁸⁵
C23	Enterprise Content Division of Dell EMC	Dell EMC; EMC (Benelux) B.V.; EMC International Company	Open Text Corporation	1,620	Application Software	Yes ⁸⁶	Yes ⁸⁷	134	365 ⁸⁸
C24	Data centers and colocation business of CenturyLink, Inc.	Lumen Technologies, Inc.	BC Partners; LongView Asset Management, LLC; Medina Capital Advisors, LLC	2,300	Integrated Telecommunication Services	Yes ⁸⁹	Yes ⁹⁰	179	n/a
C25	Safety Business of Intrado Corporation	Intrado Corporation; Apollo Global Management, Inc. ⁹¹	Stonepeak Partners LP	2,400	Application Software	Yes ⁹²	Yes ⁹³	138	n/a
C26	Technology-Enabled Benefits & Human Resources Platform of Aon plc	Aon plc	Tempo Acquisition, LLC, Blackstone Group L.P. ⁹⁴	4,800	Application Software	Yes ⁹⁵	Yes ⁹⁶	81	n/a

Exhibit 1 Notes and Sources

[1] “Divested Asset/Target,” “Seller,” “Buyer,” “Total Transaction Value (\$M),” and “Industry of Target” are respectively taken from the following fields in S&P Capital IQ Pro, unless otherwise noted: “Target/Issuer Name,” “Sellers,” “Buyers/Investors,” “Total Transaction Value (\$M),” and “Transaction Industry (MI).” To compute the observable corporate timeline, I used the announcement date (field “Announced Date”) and closing date (field “Completion Date”) as reported by S&P Capital IQ Pro.

[2] See footnote 95 in my declaration for a definition of “expected” and “observable” timelines. When I have found no public documentation on the observable timeline of a divestiture, I can nevertheless derive an expected operational timeline from the public record. Divestitures for which I was unable to identify either an expected or an observable operational timeline are denoted as “n/a.”

A1 - TikTok U.S. Application

[3] The Act appears to present Petitioners with a choice: (a) sell TikTok’s U.S. application on terms set out in the Act, or (b) be banned from operating TikTok in the U.S. See the Act, Section 2(a)(1).

[4] ByteDance’s 2017 acquisition of Musical.ly is irrelevant for this evaluation because divesting TikTok’s U.S. application would be far different than unwinding the Musical.ly transaction. Although ByteDance initially ran Musical.ly as an “independent platform” (“China’s ByteDance Buying Lip-Sync App Musical.ly for Up to \$1 Billion,” Reuters, November 10, 2017, <https://www.reuters.com/article/idUSKBN1DA0BQ/>), before relaunching TikTok in the United States in August 2018, ByteDance “abandoned the Musical.ly code base and technology, including Musical.ly’s recommendation engine, operation system, user growth, and marketing tools.” (Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10.) ByteDance integrated Musical.ly’s “user base, some music licensing agreements and other copyright agreements” with the “technology platform [...] developed by ByteDance before the Musical.ly acquisition had even occurred.” (See Petition, *TikTok Inc. et al v. CFIUS*, No. 20-1444, November 10, 2020, pp. 9-10. See also Rebecca Fannin, “The Strategy Behind TikTok’s Global Rise,” Harvard Business Review, September 13, 2019, <https://hbr.org/2019/09/the-strategy-behind-tiktoks-global-rise>.) As a result, the current TikTok app in the United States has only the barest attributes of the Musical.ly app from 2017 and there is essentially no Musical.ly app to divest.

B1 - Northeast Business

[5] Verizon would, under the agreement, “establish[] a separate entity for its local exchange and related business assets in Maine, New Hampshire and Vermont, spin[] off that new entity to Verizon’s stockholders, and merge[] it with and into FairPoint.” See “Verizon and FairPoint Agree to Merge Verizon’s Wireline Businesses in Maine, New Hampshire and Vermont,” Verizon News Archives, January 16, 2007, <https://www.verizon.com/about/news/press-releases/verizon-and-fairpoint-agree-merge-verizons-wireline-businesses-maine-new-hampshire-and-vermont>.

[6] Verizon’s access lines in Maine, Vermont and New Hampshire were all long-term holdings of Verizon. See Bob Varettoni, “Verizon Communications History,” Verizon, September 2016, https://www.verizon.com/about/sites/default/files/Verizon_History_0916.pdf.

[7] “Within 30 calendar days following the date hereof [January 15, 2007], the Cutover Planning Committee shall hold its initial meeting to commence planning and preparation for the Buyers to cease using all Transition Services and thereafter.” The start date for planning is assumed to be the last day for cutover planning, based on the 180-day timeline for the cutover plan. “On February 9, 2009, we (FairPoint) began to independently operate on our new systems.” See Transition Services Agreement by and among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>; FairPoint Communications, Inc., Form 10-Q/A for the Quarterly Period Ended September 30, 2009, <https://www.sec.gov/Archives/edgar/data/1062613/000104746910008341/a2200213z10-ka.htm>.

Exhibit 1 Notes and Sources

B2 - 14-State Divestiture

[8] The transaction “result[ed] in Frontier owning Verizon’s wireline operations in all or parts of 14 states.” *See* “California, Nevada and South Carolina Approve Frontier Acquisition of Verizon Local Wireline Operations,” Verizon News Archives, October 29, 2009, <https://www.verizon.com/about/news/press-releases/california-nevada-and-south-carolina-approve-frontier-acquisition-verizon-local-wireline-operations>.

[9] Verizon’s operations in 13 states were long-term holdings of Verizon’s corporate predecessor GTE. The other state (West Virginia) was a long-time holding of Bell Atlantic.

[10] While the parties were able to cutover the sole legacy Bell Atlantic jurisdiction (West Virginia) on or about the closing date, the cutover for the remaining GTE properties entered a lengthy transition process. Frontier announced on April 2, 2012 that “all operating, financial and human resources systems associated with its 2010 acquisition of Verizon wireline exchanges in 14 states have been successfully converted onto Frontier’s legacy systems.” *See* Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.

B3 - HawaiianTel

[11] Verizon revealed that “discussions [had] taken place” with regard to the divestment of approximately 700,000 access lines operated by Verizon Hawaii, Inc. *See* Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2003, p. 15; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2004, p. 16.

[12] Verizon’s local telephone business in Hawaii had been part of Verizon’s corporate predecessor GTE for almost 40 years. *See* “Celebrating 140 Years of Building Connections,” Hawaiian Telcom, <https://www.hawaiiantel.com/aboutus/Our-History>.

[13] “HT Communications and BearingPoint entered into a Master Service Agreement on February 4, 2005.” “The transition period has an initial nine-month term, which by amendment dated December 15, 2005, was extended to April 1, 2006.” *See* Decision and Order No. 21696, *In the Matter of the Application of Paradise Mergersub, Inc., GTE Corporation, Verizon Hawaii Inc., Bell Atlantic Communications, Inc., and Verizon Select Services Inc. for Approval of a Merger Transaction and Related Matters.*, No. 04-0140, <https://files.hawaii.gov/dcca/dca/dno/dno2005/21696.pdf>; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>.

C1 - ILEC business of Lumen Technologies, Inc.

[14] “Lumen Technologies [...] announced it has entered into a definitive agreement to sell its ILEC (incumbent local exchange carrier) business, including its consumer, small business, wholesale and mostly copper-served enterprise customers and assets, in 20 states [...]” *See* “Lumen to Sell Local Incumbent Carrier Operations in 20 States to Apollo Funds for \$7.5 Billion,” PR Newswire, August 3, 2021, <https://www.prnewswire.com/news-releases/lumen-to-sell-local-incumbent-carrier-operations-in-20-states-to-apollo-funds-for-7-5-billion-301347625.html>.

[15] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[16] “Under the TSA, Lumen actually began providing transition services upon the October 3, 2022 completion date of the Divestiture. [...] The term of services to be provided under the TSA is an average of 17 months, subject to Apollo’s right to extend the term of certain services for up to six months and to terminate early the term of any service.” *See* Lumen Technologies, Inc., Form 8-K, dated October 3, 2022, <http://pdf.secdatabase.com/1788/0001193125-22-256669.pdf>, p. 6.

Exhibit 1 Notes and Sources

C2 - Northwest operations and assets of Frontier Communications

[17] For clarity, I have augmented the name of the target as presented in S&P Capital IQ Pro by adding the geographic location of the divested asset.

[18] “Searchlight Capital Partners, L.P. [...] announced [...] that it completed the acquisition of the Northwest operations and assets of Frontier Communications [...] in partnership with WaveDivision Capital, LLC, [...] the Public Sector Pension Investment Board [...], British Columbia Investment Management Corporation [...] and Canada Pension Plan Investment Board [...].” *See* “Searchlight Capital Partners Completes the Acquisition of the Operations and Assets of Frontier Communications in the Northwest of the U.S. to form Ziplly Fiber,” PSP, May 1, 2020, <https://www.investpsp.com/en/news/searchlight-capital-partners-completes-the-acquisition-of-the-operations-and-assets-of-frontier-communications-in-the-northwest-of-the-u-s-to-form-ziplly-fiber/>.

[19] The public record that I have reviewed indicates that Frontier did not acquire the divested asset within ten years before the evaluated divestiture. Although Frontier acquired Verizon’s wireline operations in Washington, Oregon, and Idaho in the 14-State Divestiture in 2010, the asset divested in 2019 was different than those acquired in 2010. First, the divested asset included Frontier’s wireline operations in Montana, which it did not acquire from Verizon. (*See* “California, Nevada and South Carolina Approve Frontier Acquisition of Verizon Local Wireline Operations,” Verizon News Archives, October 29, 2009, <https://www.verizon.com/about/news/press-releases/california-nevada-and-south-carolina-approve-frontier-acquisition-verizon-local-wireline-operations>). Second, the divested asset included the lines that Frontier operated in Oregon and Idaho prior to the 2010 14-State Divestiture, which were subsequently integrated with the operations purchased from Verizon. (*See* “Frontier Communications Announces Sale of Operations in Washington, Oregon, Idaho, and Montana,” Frontier Communications, May 29, 2019, <https://investor.frontier.com/news/news-details/2019/Frontier-Communications-Announces-Sale-of-Operations-in-Washington-Oregon-Idaho-and-Montana-05-29-2019/default.aspx>. Citizens Communications Company, Form 10-K for the Fiscal Year Ended December 31, 2006, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/c1dd8f8d-65be-4a83-b357-0075cbe1fe54.pdf>, Exhibit 21.)

[20] Frontier committed to planning the transition of operations at least as early as July 31, 2019 (“Frontier has agreed to replicate its current IT systems.”). Frontier stated that it stopped providing the services regulated by the TSA as of October 31, 2020. *See* Testimony of Steve Weed, No. UT-190574, July 31, 2019, p. 37; Frontier Communications, Form 10-K for the Fiscal Year Ended December 31, 2020, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/6b950dad-b24b-4079-ae7e-b089a4f71e59.pdf>, F-29.

Exhibit 1 Notes and Sources

C3 - International business segment of CDK Global, Inc.

[21] “Francisco Partners [...] announced today the execution of a definitive agreement [...] to acquire CDK’s International business segment [...], a leading provider of automotive retail software solutions in EMEA and Asia, for \$1.45 billion.” See “Francisco Partners to Acquire International Business of CDK Global for \$1.45 Billion,” Francisco Partners, November 30, 2020, <https://www.franciscopartners.com/media/francisco-partners-to-acquire-international-business-of-cdk-global-for-145-billion>.

[22] Although ADP spun off CDK in 2014, this spin-off is irrelevant when evaluating CDK's 2021 divestiture of its international business. This is because, in 2021, CDK sold only one division of CDK (*i.e.*, its international business), rather than the entire entity that was spun off in 2014. Therefore, in 2021, CDK had to disentangle its international business from the rest of the entity. For this reason, the divested asset (*i.e.*, the international business) was not an asset that was acquired within ten years of the announcement date. *See* John Kirwan, "International Business of CDK Global Becomes Keyloop," MotorTrader.com, March 1, 2021, <https://www.motortrader.com/motor-trader-news/automotive-news/307888-01-03-2021>.

[23] The TSA is attached to the Share Sale and Purchase Agreement dated November 27, 2020. CDK Global, Inc. “provided limited services to Francisco Partners to assist in the integration of the International Business through February 2022.” As the precise end date is unknown, I conservatively assumed that CDK’s transition services ended on February 1, 2022. *See* CDK Global Holdings Ltd. and Concorde Bidco Ltd., Share Sale and Purchase Agreement, dated November 27, 2020, https://www.sec.gov/Archives/edgar/data/1609702/000160970221000005/cdk_q2fy21concorde-sharesa.htm; Brookfield Business Partners L.P., Brookfield Business Corporation, Form 6-K for the Month of May 2022, dated May 10, 2022, https://content.edgar-online.com/ExternalLink/EDGAR/0001104659-22-057962.html?hash=6a22c296048e3cbb7c3798faab71528dd41a7b4a071c7e69e4ed072b604cb2f3&dest=tm2213999d6_6k.htm#tm2213999d6_6k.htm.

C4 - Verizon's wireline operations in California, Texas and Florida

[24] For clarity, I have augmented the name of the target as presented in S&P Capital IQ Pro by adding the geographic location of the divested asset.

[25] Frontier completed its “acquisition of Verizon Communications, Inc. (NYSE:VZ) wireline operations providing services to residential, commercial and wholesale customers in California, Texas and Florida.” See “Frontier Communications Completes Acquisition of Verizon Wireline Operations in California, Texas and Florida,” April 1, 2016, <https://investor.frontier.com/news/news-details/2016/Frontier-Communications-Completes-Acquisition-of-Verizon-Wireline-Operations-in-California-Texas-and-Florida-04-01-2016/default.aspx>.

[26] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[27] I conservatively assumed the start of the operational timeline March 1, 2015, *i.e.*, the first day after the cutover plan support agreement was entered. I considered the end of the operational timeline, April 1, 2016, the transaction close date. The resulting 398 days are consistent with a 2019 settlement agreement stating that “Frontier had been planning the transition for more than a year[.]” See Response of Frontier California Inc. (U 1002 C) to Assigned Commissioner’s Ruling Inviting Party and Public Comments Regarding Issues Raised at Public Participation Hearings and Workshops in the Intrastate Rural Call Completion Issues Proceeding (I.14-05-012), September 20, 2016, <https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M168/K257/168257703.PDF>, Attachment A; Frontier CPED Settlement Agreement, December 19, 2019, <https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M472/K024/472024199.pdf>, p. 2.

Exhibit 1 Notes and Sources

C5 - Intellectual Property & Science business of Thomson Reuters Corporation

[28] Thomson Reuters sold its Intellectual Property & Science business which “provides comprehensive intellectual property and scientific information, decision support tools and services[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. “The newly independent company will be known as Clarivate Analytics[.]” See “Thomson Reuters Announces Definitive Agreement to Sell Its Intellectual Property & Science Business to Onex and Baring Asia for \$3.55 Billion,” PR Newswire, July 11, 2016, <https://www.prnewswire.com/news-releases/thomson-reuters-announces-definitive-agreement-to-sell-its-intellectual-property--science-business-to-onex-and-baring-asia-for-355-billion-300296352.html>; “Acquisition of the Thomson Reuters Intellectual Property and Science Business by Onex and Baring Asia Completed,” Clarivate, October 3, 2016, <https://clarivate.com/news/acquisition-thomson-reuters-intellectual-property-science-business-onex-baring-asia-completed/>.

[29] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[30] I considered the start of the operational timeline the date of the TSA, July 10, 2016. I conservatively assumed the end of the operational timeline to be July 1, 2019, because the buyer recorded “payments to Thomson Reuters under the [TSA]” during the three months ended September 30, 2019. See Clarivate Analytics PLC, Quarterly and Semi-Annual Report, as of and for the Three and Six Months Ended June 30, 2019, https://www.sec.gov/Archives/edgar/data/1764046/000114420419038016/tv526618_ex99-1.htm, pp. 9, 22; “Clarivate Analytics Reports Third Quarter 2019 Results,” Clarivate Analytics (November 6, 2019), <https://clarivate.com/news/clarivate-analytics-reports-third-quarter-2019-results/>.

C6 - Match Group, Inc.

[31] S&P Capital IQ Pro presents the target as “IAC Holdings, Inc.” and the seller as “Match Group, Inc.” For clarity, I have replaced these names by the relevant corporate predecessors: “Match Group, Inc.” and “IAC Holdings, Inc.,” respectively. See “IAC Announces Agreements to Sell Shares relating to Match Group in Connection with Separation of Match Group and IAC,” News Release Details, June 9, 2020, <https://ir.iac.com/news-releases/news-release-details/iac-announces-agreements-sell-shares-relating-match-group>.

[32] “Since Match Group’s initial public offering in 2015, the company has more than doubled subscribers and revenue. Match Group’s flagship product, Tinder, is the highest grossing non-gaming app worldwide, with a global presence.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. See “IAC and Match Group Complete Full Separation,” IAC, July 1, 2020, <https://www.iac.com/press-releases/iac-and-match-group-complete-full-separation>.

[33] The public record that I have reviewed also indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. Match.com was acquired by TMCS (Ticketmaster Online-CitySearch Inc.) in June 1999 (*i.e.*, more than ten years before this divestiture’s announcement date). In 2003 (still more than ten years before this divestiture’s announcement date), IAC acquired TMCS, and following Match.com’s IPO on November 24, 2015, IAC retained a significant stake in the company. See “25 Year Innovator,” IAC, <https://www.iac.com/history>; “IAC and Match Group Announce Closing of Initial Public Offering,” IAC, November 24, 2015, <https://www.iac.com/press-releases/iac-and-match-group-announce-closing-of-initial-public-offering>.

[34] I considered the start of the operational timeline the date of the TSA, June 30, 2020. I conservatively assumed the end of the operational timeline to be July 1, 2022, because the seller recorded revenues “from IAC for services provided to IAC under the transition services agreement” during the three-month period ended September 30, 2022. See Transition Services Agreement by and between IAC/InterActiveCorp and IAC Holdings, Inc., dated June 30, 2020, https://www.sec.gov/Archives/edgar/data/1800227/000110465920080610/tm2022502d7_ex10-1.htm; Match Group, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2022, dated November 4, 2022, <https://www.sec.gov/Archives/edgar/data/891103/000089110322000095/mtch-20220930.htm>, p. 27.

Exhibit 1 Notes and Sources

C7 - Vimeo, Inc.

[35] The divestiture involved the spin-off of Vimeo, “the video platform enabling any business in the world from Fortune 500s to local shops to harness the power of video in countless ways to better create, communicate, and collaborate.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “IAC Completes Spin-Off Of Vimeo,” IAC, May 25, 2021, <https://www.iac.com/press-releases/iac-completes-spin-off-of-vimeo>.

[36] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[37] I considered the start of the operational timeline the date of the TSA, May 24, 2021. I made the conservative assumption that the end of the operational timeline is January 1, 2023 because, as of at least January 1, 2023, IAC continued to receive fees “for services rendered pursuant to the transition services agreement.” *See* Transition Services Agreement by and between IAC/InterActiveCorp and Vimeo, Inc., dated May 24, 2021, https://www.sec.gov/Archives/edgar/data/1837686/000110465921073207/tm2117737d1_ex10-3.htm; IAC Inc., Form 10-Q for the Quarterly Period Ended March 31, 2023, <https://www.sec.gov/Archives/edgar/data/1800227/000180022723000016/iaci-20230331.htm>.

C8 - SolarWinds MSP

[38] S&P Capital IQ Pro presents the target as “N-able, Inc.,” which is the name of the spun-off company. For clarity, I have replaced this by the name of the SolarWinds division that existed prior to the spin-off.

[39] SolarWinds spun off its Managed Service Provider (“MSP”) business into a separate company called N-able. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* Kara Carlson, “SolarWinds Spins Off Business Unit into New Company, N-able,” TechXplore, July 21, 2021, <https://techxplore.com/news/2021-07-solarwinds-business-company-n-able.html>.

[40] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture. I note that SolarWinds’ 2013 acquisition of a different company that was also called “N-able” is irrelevant for this evaluation. Following this 2013 acquisition, SolarWinds integrated the assets of N-able with the assets of another company that SolarWinds acquired in 2016 (LOGICnow) to create “SolarWindsMSP.” Then, in 2021, SolarWinds spun off “SolarWindsMSP” as a new entity, which SolarWinds named “N-able.” *See* Stefanie Hammond, “Happy anniversary to me!,” N-able, November 24, 2021, <https://www.n-able.com/fr/blog/happy-anniversary-to-me>.

[41] The TSA was dated as of July 16, 2021, and the transition services were expected to end on December 31, 2022 (“The transition services agreement will terminate on the expiration of the term of the last service provided under it, which SolarWinds anticipates to be on or around December 31, 2022.”). *See* Transition Services Agreement by and between SolarWinds Corporation and N-Able, Inc., dated July 16, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000162828021014064/exhibit101-swinxable8xk.htm>;

SolarWinds Corporation, Form 10-K for the Fiscal Year Ended December 31, 2021, <https://www.sec.gov/Archives/edgar/data/1739942/000173994222000020/swi-20211231.htm>, p. F-36.

Exhibit 1 Notes and Sources

C9 - Software Business of Hewlett Packard Enterprise

[42] Micro Focus International “purchase[d] [...] Hewlett Packard Enterprise’s software business for £6.8bn.” I used the U.S. dollar value of \$9.00 billion as reported by S&P Capital IQ Pro. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “UK Tech Giant Micro Focus Plunges in Value as Shares Crash,” BBC, March 19, 2018, <https://www.bbc.com/news/business-43457024>.

[43] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[44] “The initial term of the Transition Services Agreement will be nine months, and each party in certain circumstances may extend the term of services it will receive for up to two three-month periods (for a total term of up to 15 months).” *See* Transition Services Agreement by and between Hewlett Packard Enterprise Company and Seattle SpinCo, Inc., dated September 1, 2017, https://www.sec.gov/Archives/edgar/data/1645590/000156761917001826/s001851x1_ex2-3.htm; Seattle SpinCo, Inc. and Micro Focus International plc, Form 42B3, dated August 15, 2017, https://www.sec.gov/Archives/edgar/data/1359711/000156761917001747/s001838x1_424b3.htm#t149%7Dt149, p. 219.

C10 - ADP Dealer Services, Inc.

[45] “Automatic Data Processing, Inc. (ADP) completed the distribution to its stockholders of all of the issued and outstanding common stock of CDK Global, Inc. in a tax-free spin-off. The distribution completes the spin-off by ADP of its automotive dealer services business.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “ADP Completes Spin-Off of Automotive Dealer Services Business,” Paul Weiss, September 30, 2014, <https://www.paulweiss.com/practices/transactional/corporate/news/adp-completes-spin-off-of-automotive-dealer-services-business?id=18827>.

[46] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[47] I considered the start of the operational timeline the date of the TSA, September 29, 2014. I considered the end of the operational timeline September 30, 2015, the last date of the transitional period “pursuant to the transition services agreement” with ADP. *See* CDK Global, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2014, https://www.sec.gov/Archives/edgar/data/1609702/000160970214000006/cdk_q1fy1510-q.htm, p. 34; CDK Global, Inc., Form 10-Q for the Quarterly Period Ended December 31, 2015, https://www.sec.gov/Archives/edgar/data/1609702/000160970216000037/cdk_q2fy1610-q.htm, p. 7.

C11 - Website security business of Symantec Corporation

[48] S&P Capital IQ Pro presents the seller as “Gen Digital Inc.” For clarity, I have replaced this by the name of Gen Digital’s corporate predecessor, Symantec Corporation.

[49] DigiCert announced that it acquired “Symantec’s Website Security business.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* John Merrill, “DigiCert to Acquire Symantec’s Website Security Business,” DigiCert, August 2, 2017, <https://www.digicert.com/blog/digicert-to-acquire-symantec-website-security-business>.

[50] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[51] From the Purchase Agreement between Symantec and DigiCert: “Unless otherwise agreed by Arion (refers to DigiCert) and Sphinx (refers to Symantec) or set forth in the Preliminary Transition Service Schedules, no Transition Period will last for more than 12 months following the Closing Date (excluding any extensions made to the Transition Period in accordance with the terms of the Transition Services Agreement).” From the 10-Q for the Quarterly Period Ended December 29, 2017: “The services under the TSA commenced with the close of the transaction and expire at various dates through fiscal 2019, with extension options.” *See* Purchase Agreement by and among Symantec Corporation, DigiCert Parent, Inc., and DigiCert, Inc., dated August 2, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939917000016/a092917exhibit21.htm>, pp. 111-112; Symantec Corporation, Form 10-Q for the Quarterly Period Ended December 29, 2017, <https://www.sec.gov/Archives/edgar/data/849399/000084939918000004/symc122917-10q.htm>, p. 14.

Exhibit 1 Notes and Sources

C12 - Software Portfolio of IBM Corp.

[52] HCL Technologies agreed to buy select software products from IBM. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “HCL Technologies to Buy IBM Software Products in \$1.8 Billion Deal,” Nikkei Asia, December 7, 2018, <https://asia.nikkei.com/Business/Companies/HCL-Technologies-to-buy-IBM-software-products-in-1.8-billion-deal>.

[53] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[54] For the lower bound of the operational timeline, I conservatively assumed that the start date is January 31, 2019 because HCL Tech announced in January 2019 that “HCL is working on a smooth transition plan.” As the end date, I conservatively used the date of the deal close, June 30, 2019. For the upper bound, I conservatively used 365 days because IBM stated that “HCL can renew certain [transition] services up to an additional year.” *See* “HCL Announces Acquisition of Select IBM Products Frequently Asked Questions,” Products & Platforms, https://www.hcltech.com/sites/default/files/documents/inline-migration/general_faq_jan_2019.pdf, p. 3; IBM Corporation, Form 10-Q for the Quarter Ended September 30, 2019, <https://www.sec.gov/Archives/edgar/data/51143/000155837019009324/ibm-20190930x10q.htm>, p. 52.

C13 - GoTo subsidiary of Citrix Systems, Inc.

[55] S&P Capital IQ Pro presents the seller as “GoTo Group Inc.” For clarity, I have replaced this by the name of GoTo Group’s corporate predecessor, LogMeIn Inc.

[56] The divested asset is “a unit of Citrix Systems Inc (CTXS.O) that makes software products such as GoToMeeting[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* Liana B. Baker, “LogMeIn to Merge with Citrix’s GoTo Unit in All-Stock Deal,” Yahoo Finance, July 26, 2016, <https://finance.yahoo.com/news/logmein-merge-citrixs-goto-unit-002645133.html>.

[57] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[58] I considered the start of the operational timeline the date of the TSA, January 31, 2017. I considered the end of the operational timeline December 31, 2017, the date when the company stated that “the transition services are substantially complete.” *See* LogMeIn, Inc., Form 10-K for the Fiscal Year ended December 31, 2016, <https://www.sec.gov/Archives/edgar/data/1420302/000119312517063977/d301311d10k.htm>, p. 90; LogMeIn, Inc., Form 10-K for the Fiscal Year ended December 31, 2017, <https://www.sec.gov/Archives/edgar/data/1420302/000119312518050503/d506130d10k.htm>, p. 71.

Exhibit 1 Notes and Sources

C14 - Enterprise security business of Symantec Corporation

[59] S&P Capital IQ Pro presents the seller as “Gen Digital Inc.” For clarity, I have replaced this by the name of Gen Digital’s corporate predecessor, Symantec Corporation.

[60] Broadcom announced plans to “acquire the enterprise security business of Symantec Corporation[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. “[Symantec Corporation] is now NortonLifeLock Inc., but its previous name will live on since Broadcom owns the rights to the Symantec name for the company’s previous enterprise security products.” *See* “Broadcom to Acquire Symantec Enterprise Security Business for \$10.7 Billion in Cash,” Broadcom, August 8, 2019, <https://investors.broadcom.com/news-releases/news-release-details/broadcom-acquire-symantec-enterprise-security-business-107>; Duncan Riley, “Symantec Is Now NortonLifeLock as Broadcom Closes Purchase of Its Enterprise Business,” SiliconANGLE, November 5, 2019, <https://siliconangle.com/2019/11/05/symantec-now-nortonlifelock-broadcom-completes-acquisition-enterprise-business/>.

[61] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[62] I considered the start of the operational timeline August 8, 2019, the date of the Asset Purchase Agreement to which the TSA was attached. I conservatively considered the end of the operational timeline July 2, 2020 because the parties reported having incurred transition services costs “during the three [...] months ended October 2, 2020.” *See* Broadcom Inc., Symantec Corporation, Asset Purchase Agreement by and Between Broadcom Inc. and Symantec Corporation, dated August 8, 2019, <https://www.sec.gov/Archives/edgar/data/1730168/000119312519217369/d790567dex21.htm>; NortonLifeLock Inc., Form 10-Q for the Quarterly Period Ended October 2, 2020, <https://www.sec.gov/Archives/edgar/data/849399/000084939920000011/nlok-20201002.htm>, p. 10.

C15 - Yahoo’s operating business

[63] Verizon acquired “the operating business of Yahoo! Inc.” and “combined these assets with its existing AOL business to create a new subsidiary[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary,” Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsidiary>.

[64] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

[65] I conservatively considered the start of the operational timeline July 25, 2016, because “the Yahoo transaction was announced” in July 2016. I considered the end of the operational timeline June 13, 2017, the date when “Oath beg[an] operation[.]” (Oath CEO “has been leading integration planning teams since the Yahoo transaction was announced in July 2016”). *See* “Verizon Completes Yahoo Acquisition, Creating a Diverse House of 50+ Brands Under New Oath Subsidiary,” Verizon, June 13, 2017, <https://www.verizon.com/about/news/verizon-completes-yahoo-acquisition-creating-diverse-house-50-brands-under-new-oath-subsidiary>.

C16 - Fiber-optic network business of XO Holdings, Inc.

[66] Verizon agreed to purchase XO Communications’ fiber business. “In February 2016, we entered into a purchase agreement to acquire XO Holdings’ wireline business (XO), which owned and operated one of the largest fiber-based IP and Ethernet networks in the U.S.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Verizon Continues Focus on Network Superiority with Agreement to Purchase XO Communications’ Fiber Business,” Verizon News Archives, February 22, 2016, <https://www.verizon.com/about/news/verizon-continues-focus-network-superiority-agreement-purchase-xo-communications-fiber>; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2018, <https://www.sec.gov/Archives/edgar/data/732712/000073271219000012/a2018q410-k.htm>, p. 9.

[67] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

Exhibit 1 Notes and Sources

C17 - Mobile and web assets of Weather Channel LLC

[68] “The deal doesn’t include the TV operations, but is focused on the Weather Company’s range of digital weather information assets including smartphone apps and websites as well as data sets.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* Arik Hesseldahl, “IBM in Deal for Weather Channel Digital Assets,” Vox, October 28, 2015, <https://www.vox.com/2015/10/28/11620118/ibm-in-deal-for-weather-channel-digital-assets>.

[69] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

C18 - Acxiom marketing solutions business

[70] Acxiom Corporation divested its Acxiom Marketing Solutions segment (“AMS”) and changed its brand name to LiveRamp after the sell-off. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* Zacks Equity Research, “Acxiom to Divest AMS to Interpublic Group for \$2.3 Billion,” Yahoo Finance, July 3, 2018, <https://finance.yahoo.com/news/acxiom-divest-ams-interpublic-group-143302074.html>.

[71] The public record that I have reviewed indicates that the seller did not acquire the divested asset within ten years before the evaluated divestiture.

C19 - Xperi Inc.

[72] Xperi Holding Corporation spun off the company’s product business, Xperi Inc. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* Xperi Holding Corp, “Xperi Announces Details for Completion of Separation,” September 8, 2022, <https://www.sec.gov/Archives/edgar/data/1803696/000119312522240678/d693283dex991.htm>.

[73] Xperi (formerly Tessera Holding Corporation) acquired the product business of DTS, Inc in December 2016, *i.e.*, six years before this divestiture. *See* “Tessera Completes Acquisition of DTS,” Business Wire, December 1, 2016, <https://www.businesswire.com/news/home/20161201005268/en/Tessera>; “Tessera Holding Corporation Announces Name Change to Xperi Corporation,” Xperi, February 22, 2017, <https://investor.xperi.com/news/news-details/2017/Tessera-Holding-Corporation-Announces-Name-Change-to-Xperi-Corporation/default.aspx>.

[74] While I have found neither the precise start date nor the precise end date of the operational timeline from public documents, I was able to estimate the operational timeline by using conservative proxy dates for both. As the start date, I used July 1, 2020, which is the first day following the month in which Xperi publicly announced its intention to divest its asset (June 2020). Using this date as the start of the operational timeline is conservative because public announcements typically occur following internal operational planning. As the end date, I used October 22, 2022, date of the first amendment to the TSA. This date is conservative as the implementation of the TSA is likely to continue after its amendment date. *See* Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2023, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001788999/0768588f-717f-4908-a897-745524c9f289.pdf>, pp. 51-52; Xperi Inc., Form 10-K for the Fiscal Year Ended December 31, 2022, <https://www.sec.gov/ix?doc=/Archives/edgar/data/1788999/000095017023006053/xper-20221231.htm>, p. 105.

Exhibit 1 Notes and Sources

C20 - Cars.com Inc.

[75] Cars.com spun off from its parent company TEGNA. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Cars.com Completes Spin-off from Parent Company TEGNA,” Cars.com, June 1, 2017, <https://www.cars.com/articles/carscom-completes-spin-off-from-parent-company-tegna-1420695567172/>.

[76] Gannett, the corporate predecessor of TEGNA, acquired Cars.com in 2014, *i.e.*, three years before this divestiture. *See* Veronica Garabelli, “Gannett Acquires Cars.com for \$1.8 Billion,” Virginia Business, October 1, 2014, <https://www.virginiabusiness.com/article/gannett-acquires-cars-com-for-1-8-billion/>; “Separation of Gannett into Two Public Companies Completed,” TEGNA, June 29, 2015, <https://www.tegna.com/separation-of-gannett-into-two-public-companies-completed/>.

[77] TEGNA and Cars.com entered into a TSA on May 31, 2017, pursuant to which TEGNA agreed to “provide certain services to Cars.com on an interim and transitional basis, not to exceed 24 months.” *See* Transition Services Agreement by and between TEGNA Inc. and Cars.com Inc., dated May 31, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000119312517196074/d514170dex101.htm>; TEGNA Inc., Form 10-Q for the Quarterly Period ended September 30, 2017, <https://www.sec.gov/Archives/edgar/data/39899/000003989917000041/tgna-20170930x10q.htm>, p. 20.

C21 - Products business of FireEye, Inc.

[78] S&P Capital IQ Pro presents the seller as “Mandiant, Inc.” For clarity, I have replaced this by the name of Mandiant’s corporate predecessor, FireEye Inc.

[79] S&P Capital IQ Pro presents the buyer as “Musarubra US LLC.” For clarity, I have replaced this by the name of the private equity firm holding Musarubra, Symphony Technology Group. *See* Corporate website of Skyhigh Security, careers section, <https://careers.skyhighsecurity.com/>.

[80] FireEye, Inc. (now Mandiant, Inc.) “announced it has entered into a definitive agreement to sell the FireEye Products business [...] to a consortium led by Symphony Technology Group[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion,” Mandiant, June 2, 2021, <https://www.mandiant.com/company/press-releases/fireeye-announces-sale-fireeye-products-business-symphony-technology-group>.

[81] “Through this transaction, [FireEye] undoes its 2014 acquisition, which brought Mandiant solutions and FireEye products together.” *See* Zacks Equity Research, “FireEye Rebrands as Mandiant (FEYE) After Product Biz Sell-Off,” Nasdaq, October 5, 2021, <https://www.nasdaq.com/articles/fireeye-rebrands-as-mandiant-feye-after-product-biz-sell-off-2021-10-05>.

[82] On June 2, 2021, FireEye said it would enter into a TSA at closing (“[FireEye] at closing will enter into agreements [which] include [...] a transition services agreement”). “The transition period is expected to be approximately 12 to 18 months after the sale closes.” *See* “FireEye Announces Sale of FireEye Products Business to Symphony Technology Group for \$1.2 Billion,” Mandiant, June 2, 2021, <https://www.mandiant.com/company/press-releases/fireeye-announces-sale-fireeye-products-business-symphony-technology-group>; FireEye, Inc., Form 10-Q for the Quarterly Period ended June 30, 2021, <https://www.sec.gov/Archives/edgar/data/1370880/000137088021000033/feye-20210630.htm>, p.12.

Exhibit 1 Notes and Sources

C22 - VMware LLC

[83] Dell spun off its equity ownership of VMware Inc. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Dell Technologies Announces Completion of VMware Spin-off,” Dell Technologies, November 1, 2021, <https://www.dell.com/en-us/dt/corporate/newsroom/announcements/detailpage.press-releases~usa~2021~11~20211101-dell-technologies-announces-completion-of-vmware-spin-off.htm#/filter-on/Country:en-us>.

[84] Dell acquired VMware in 2015, *i.e.*, six years before this divestiture. *See* Ron Miller and Alex Wilhelm, “Dell Is Spinning Out VMware in a Deal Expected to Generate Over \$9B for the Company,” TechCrunch, April 14, 2021, <https://techcrunch.com/2021/04/14/dell-is-spinning-out-vmware-in-a-deal-expected-to-generate-over-9b-for-the-company/>.

[85] “In connection with the Spin-Off, on November 1, 2021, Dell entered into a [...] Transition Services Agreement[.]” “Transition services may be provided for up to one year.” “Costs associated with [the TSA] were immaterial for the three and nine months ended October 28, 2022.” *See* Dell Technologies Inc., Form 8-K, dated October 29, 2022, <https://investors.delltechnologies.com/static-files/072b94f3-090e-4891-a825-0014a787b6c9>, p. 4; Dell Technologies Inc., Form 10-Q for the Quarterly Period Ended October 28, 2022, <https://www.sec.gov/Archives/edgar/data/1571996/000157199622000044/dell-20221028.htm>, pp. 15, 49.

C23 - Enterprise Content Division of Dell EMC

[86] Dell EMC’s Enterprise Content Division was a suite of product families, including Documentum™, InfoArchive™, and LEAP™. The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “OpenText Signs Definitive Agreement to Acquire Dell EMC’s Enterprise Content Division, including Documentum,” PR Newswire, September 12, 2016, <https://www.prnewswire.com/news-releases/opentext-signs-definitive-agreement-to-acquire-dell-emcs-enterprise-content-division-including-documentum-300326059.html>.

[87] Dell acquired EMC in 2016, *i.e.*, the same year of this divestiture. *See* Noreen Seebacher, “OpenText Acquires Dell EMC’s Enterprise Content Division, Including Documentum,” CMSWire, September 12, 2016, <https://www.cmswire.com/information-management/opentext-acquires-dell-emcs-enterprise-content-division-including-documentum/>.

[88] “Transition services may be provided for up to one year, with an option to renew after that period.” *See* Dell Technologies Inc., Form 10-K for the Fiscal Year Ended February 2, 2018, <https://investors.delltechnologies.com/static-files/9d4aca86-7fd6-4b4f-ab4b-4895fa562826>, p. 104.

C24 - Data centers and colocation business of CenturyLink, Inc.

[89] CenturyLink sold its data centers and colocation business, and will continue to “focus on offering customers a wide range of IT services and solutions[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “CenturyLink Reaches Agreement to Sell Data Centers and Colocation Business to a Consortium Led by BC Partners and Medina Capital,” Lumen, November 4, 2016, <https://ir.lumen.com/news/news-details/2016/CenturyLink-reaches-agreement-to-sell-data-centers-and-colocation-business-to-a-consortium-led-by-BC-Partners-and-Medina-Capital/default.aspx>.

[90] “What these new venture partners are getting for their \$2.15 billion plus stock is Savvis, which CenturyLink acquired in 2011 [*i.e.*, five years before this divestiture] in a \$2.5 billion cash + stock deal.” *See* Scott III Fulton, “CenturyLink Sells Its Colo Business to Fund Level 3 Deal,” Data Center Knowledge, November 4, 2016, <https://www.datacenterknowledge.com/investing/centurylink-sells-its-colo-business-to-fund-level-3-deal>.

Exhibit 1 Notes and Sources

C25 - Safety Business of Intrado Corporation

[91] S&P Capital IQ Pro presents the seller as “Apollo Global Management, Inc.” For clarity, I have added “Intrado Corporation,” the specific corporation controlled by Apollo that divested its Safety Business.

[92] The Safety Business of Intrado represents a separate business unit that “delivers critical emergency data over a highly reliable, secure, standards-based network[.]” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Stonepeak to Acquire Safety Business from Intrado,” Intrado, September 16, 2022, <https://www.intrado.com/news-releases/stonepeak-acquire-safety-business-intrado>.

[93] In 2017, Apollo Global Management, LLC acquired West Corporation (rebranded to Intrado in 2019), *i.e.*, five years before this divestiture. *See* “West Corporation and Affiliates of Certain Funds Managed by Affiliates of Apollo Global Management Announce the Closing of the Previously Announced Transaction,” West, October 10, 2017, <https://ir.west.com/news-releases/news-release-details/west-corporation-and-affiliates-certain-funds-managed-affiliates>; “West Corporation Announces Rebrand to Intrado,” West (June 25, 2019), <https://westcorporation.gcs-web.com/news-releases/news-release-details/west-corporation-announces-rebrand-intrado>.

C26 - Technology-Enabled Benefits & Human Resources Platform of Aon

[94] S&P Capital IQ Pro presents the seller as “Tempo Acquisition LLC.” For clarity, I have added the “Blackstone Group,” the name of its affiliated co-investor. *See* Foley Trasimene Acquisition Corp. and others, Proxy Statement/Prospectus/Consent Solicitation Statement, dated June 4, 2021, <https://www.sec.gov/Archives/edgar/data/1844744/000119312521182145/d128085d424b3.htm>.

[95] “The business is a leader in benefits administration and cloud-based HR services serving 19 million workers (approximately 15 percent of the U.S. working population) and their families across 1,400 clients.” The public record that I have reviewed indicates that a geographic market segmentation was not necessary to define the divested asset. *See* “Blackstone Completes Acquisition of Aon Hewitt’s Technology-Enabled Benefits & Cloud-Based HR Service Platform,” Blackstone, May 1, 2017, <https://www.blackstone.com/news/press/blackstone-completes-acquisition-of-aon-hewitt-s-technology-enabled-benefits-cloud-based-hr-service-platform/>.

[96] “[Aon Plc completed a merger with Hewitt Associates in October 2010[.] [...] The transaction, announced Feb. 10, essentially unwinds the 2010 Hewitt deal, as benefits outsourcing represents that business’ most profitable division[.]” The 2010 deal occurred seven years before this divestiture. *See* Matthew Rybaltowski, “Aon Refocuses Approach With HR Admin Unit Sale to Blackstone,” S&P Global, February 16, 2017, <https://www.spglobal.com/marketintelligence/en/news-insights/trending/rf3wi6dxjmdw7ok-jjiyia2>.

Appendix A

RANDAL S. MILCH
 Chilmark, MA rsmilch@gmail.com

Randal S. Milch is a seasoned corporate executive and strategic advisor, with particular expertise in cybersecurity, national security and corporate governance. At Verizon, he was responsible for developing and articulating the company's legal, public policy, cybersecurity, national security and government affairs strategies, and reporting to the board of directors. Randy has testified before committees of Congress and has organized and led significant public policy campaigns relating to state and federal legislation and critical transactions. He has most recently developed, and now directs, a cutting-edge academic program seeking to bridge the gaps between technical and non-technical cybersecurity professionals.

EXPERIENCE

NEW YORK UNIVERSITY SCHOOL OF LAW

PROFESSOR OF LAW FROM PRACTICE

2018-PRESENT

- Faculty Co-Director, NYU Master of Science in Cybersecurity Risk and Strategy Program
- Developed interdisciplinary *Cybersecurity Law and Technology* class for law students and engineering students

CO-CHAIR, NYU CENTER FOR CYBERSECURITY

2018-PRESENT

- Responsible for strategic direction and supervision of Center dedicated to interdisciplinary research in cybersecurity issues, to the development of the next generation of leaders literate in the engineering, law and policy of cybersecurity, and to the creation of public and private convenings of business, government and academic leaders seeking solutions to cybersecurity issues.

DISTINGUISHED FELLOW, REISS CENTER ON LAW AND SECURITY

2015-PRESENT

SATO TECHNOLOGIES CORP.

MEMBER, BOARD OF DIRECTORS

2023-PRESENT

xMENTIUM, INC.

MEMBER, ADVISORY BOARD

2021-PRESENT

RiskQ INC.**ADVISOR, MEMBER BOARD OF DIRECTORS****2019-2024****TEXT IQ, INC.****DOMAIN ADVISOR AND MEMBER, BOARD OF DIRECTORS****2017-2021****THE ANALYSIS GROUP****MEMBER, BOARD OF DIRECTORS****2016-PRESENT****COLUMBIA LAW SCHOOL****LECTURER IN LAW****2016**

- Co-taught *The Media Industries: Public Policy and Business Strategy* with Prof. Jonathan Knee of Columbia Business School.

VERIZON COMMUNICATIONS INC.**EXECUTIVE VICE PRESIDENT, STRATEGIC POLICY ADVISOR TO THE CHAIR AND CEO 2014-2015**

- Responsible for overseeing strategic policy initiatives for Verizon.

EXECUTIVE VICE PRESIDENT, PUBLIC POLICY, AND GENERAL COUNSEL 2008-2014

- Responsible for public policy, legal, compliance, regulatory, government affairs and security organizations.
- Senior cleared executive at Verizon responsible for national security matters; directed corporate cyber-policy; and chaired Executive Security Council, which is responsible for information security across all Verizon entities.
- Led negotiations for major corporate transactions, including Verizon's \$130 billion purchase of Vodafone's 45% stake in Verizon Wireless.
- Managed Verizon's corporate strategy on high-profile issues including NSA domestic surveillance, major transactions, net neutrality and the Snowden leaks.

SENIOR VICE PRESIDENT AND GENERAL COUNSEL, VERIZON BUSINESS 2006-2008

- Responsible for a team of 230 attorneys and all legal and public affairs issues for Verizon's global enterprise business, including national security matters.

SENIOR VICE PRESIDENT AND GENERAL COUNSEL, VERIZON TELECOM 2000-2006

- Responsible for a team of 90 lawyers and all legal issues affecting Verizon's wireline businesses in 29 states.
- Responsible for state regulatory matters.
- Advised Verizon's wireline businesses on all of their legal and public policy issues.

VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL (BELL ATLANTIC) 1997-2000

- Responsible for all regulatory issues in the former NYNEX jurisdictions (New York and New England).
- Responsible for implementation of all aspects of the 1996 Telecommunications Act, including competition provisions.
- Developed and litigated the case before the New York Public Service Commission that resulted in Bell Atlantic-New York becoming the first Incumbent Local Exchange Carrier in the nation to be allowed to enter the long distance and enterprise markets.

VICE PRESIDENT AND ASSOCIATE GENERAL COUNSEL (BELL ATLANTIC) 1995-1997

- Responsible for implementation of the 1996 Telecommunications Act across the seven Bell Atlantic jurisdictions.

VICE PRESIDENT AND GENERAL COUNSEL (BELL ATLANTIC-MARYLAND) 1994-1995

- Responsible for all legal and regulatory issues in Maryland.

REGULATORY ATTORNEY (BELL ATLANTIC-MARYLAND) 1993-1994

- Responsible for regulatory litigation before the Maryland Public Service Commission.

DONOVAN, LEISURE, NEWTON AND IRVINE LLP**PARTNER (and previously Associate) 1986-1993**

- Litigated complex federal cases and international arbitrations.

JUDICIAL CLERKSHIP**HONORABLE CLEMENT F. HAYNSWORTH, JR., CHIEF JUDGE EMERITUS,
UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT 1985-1986**

PUBLICATIONS & CONGRESSIONAL TESTIMONY

“In a Landscape Crawling with Regulation, Lawyers Can Mitigate Cyber Risk” in *Guiding Cybersecurity From the Boardroom* (D.Hechler, ed. TAG Cyber 2023). <https://tag-cyber.com/advisory/publications/guiding-cybersecurity-from-the-boardroom>

“Hack-to-Patch by Law Enforcement is a Dangerous Practice” (with Ed Amoroso). *Just Security* (April 30, 2021). <https://www.justsecurity.org/75955/hack-to-patch-by-law-enforcement-is-a-dangerous-practice/>

“What’s Good for Litigation Isn’t Necessarily Good for Cybersecurity.” *Lawfare* (Mar. 5, 2021). <https://www.lawfareblog.com/whats-good-litigation-isnt-necessarily-good-cybersecurity>

“A New Decade and New Cybersecurity Orders at the FTC” (with Sam Bieler). *Lawfare* (Jan. 29, 2020). <https://www.lawfareblog.com/new-decade-and-new-cybersecurity-orders-ftc>

“Cybersecurity in One Voice: Leveraging CISA Programming to Improve FTC Cybersecurity Enforcement” (with Sam Bieler). *Lawfare* (Dec. 5, 2019). <https://www.lawfareblog.com/cybersecurity-one-voice-leveraging-cisa-programming-improve-ftc-cybersecurity-enforcement>

“How Much is Data Security Worth?” (with Almudena Arcelus and Brian Ellman). *The SciTech Lawyer* (The American Bar Association, Spring 2019).

“Some Concerns with Privacy as A Framework for Cybersecurity” in *Privacy and Cyber Security on the Books and on the Ground* (Pernice & Pohle eds., Alexander von Humboldt Institute for Internet and Society 2018). <https://www.hiig.de/wp-content/uploads/2018/09/Pernice-Pohle-eds.-2018-Privacy-and-Cyber-Security-on-the-Books-and-on-the-Ground.pdf>

“First Legislative Step in the IoT Security Battle.” *Lawfare* (Aug. 4, 2017). <https://www.lawfareblog.com/first-legislative-step-iot-security-battle>

“Q&A: Privacy and Cybersecurity: The Corporate Perspective.” The Analysis Group (Jan. 2017). <http://www.analysisgroup.com/privacy-cybersecurity-corporate-perspective/>

“Cyber Insurance as a Way to Reduce Cyber Risk.” Before the President’s Commission on Enhancing National Cybersecurity, May 16, 2016.

“Public Service Residency in Lieu of the Third Year of Law School” (with Sam Estreicher) in *Beyond Elite Law: Access to Civil Justice in America* (Estreicher & Radice eds., Cambridge Univ. Press 2016).

“From the War Room to the Board Room? Effectively Managing Cyber Risk without Joining the Front Lines.” (with Zachary Goldman) The Center on Law and Security, New York University School of Law, June 2015.

“An Examination of Competition in the Wireless Market.” Before the United States Senate, Committee on the Judiciary, Subcommittee on Antitrust, Competition Policy and Consumer Rights, February 26, 2014.

“Samsung vs. Apple Needs an Obama Intervention.” Commentary, *The Wall Street Journal*, July 23, 2013.

“Cut Red Tape Tying up E-Medicine.” Op-ed, Politico, January 24, 2013.

“The Verizon/Cable Deals: Harmless Collaboration or a Threat to Competition and Consumers?” Before the United States Senate, Committee on the Judiciary, Subcommittee on Antitrust, Competition Policy and Consumer Rights, March 21, 2012.

“Cell Phone Text Messaging Rate Increases and the State of Competition in the Wireless Market.” Before the United States Senate, Committee on the Judiciary, Subcommittee on Antitrust, Competition Policy and Consumer Rights, June 16, 2009.

EDUCATION

NEW YORK UNIVERSITY SCHOOL OF LAW

JURIS DOCTOR, *CUM LAUDE*, ARTICLES EDITOR, N.Y.U. LAW REVIEW, ORDER OF THE COIF 1985

YALE UNIVERSITY

BACHELOR OF ARTS IN HISTORY 1980

SERVICE

Commissioner, Dukes County Commission (current)
American Law Institute, Member (current)
New York University School of Law, Life Trustee, Board of Trustees (current)
Equal Justice Works, Chair, Board of Directors
The Constitutional Sources Project, Board of Directors
National Veterans Legal Services Program, Board of Directors

Appendix B

I. EXAMPLES OF VERIZON'S DIVESTITURES OF HIGHLY INTEGRATED ASSETS

1. *HawaiianTel (2005)*

1. The divestiture of Verizon's local telephone business in Hawaii in 2005, which had been part of Verizon's corporate predecessor GTE for almost 40 years,¹ demonstrates that even relatively small divestitures of integrated assets are complex, unpredictable, and lengthy projects. The HawaiianTel divestiture spanned 751 days between Verizon's disclosure of deal discussions and the final operational cutover. Of those 751 days, the corporate timeline represented 417 days² and the operational timeline represented at least 422 days (from the time HawaiianTel hired BearingPoint on February 4, 2005, to aid in establishing back-office support systems to the final operational cutover on April 1, 2006).^{3,4}

2. The corporate timeline for the HawaiianTel divestiture began no later than March 12, 2004, when Verizon revealed that "discussions [had] taken place" with regard to the divestment of approximately 700,000 access lines operated by Verizon Hawaii, Inc.⁵ This represented approximately 1.5 percent of Verizon's landlines.⁶ A definitive agreement between Verizon and the Carlyle Group was signed

¹ See "Celebrating 140 Years of Building Connections," Hawaiian Telcom, <https://www.hawaiiantel.com/aboutus/Our-History>. Verizon was created by the merger of Bell Atlantic with GTE in 2000. Both parties brought with them their long-held legacy wireline assets. See "Bell Atlantic and GTE Complete Their Merger and Become Verizon Communications," Verizon News Archives, June 30, 2000, <https://www.verizon.com/about/news/press-releases/bell-atlantic-and-gte-complete-their-merger-and-become-verizon-communications>.

² The corporate timeline began on March 12, 2004 (when Verizon announced that it had been in divestment discussions), and it ended with the deal closing on May 2, 2005—representing a total of 417 days. See Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2003, p. 15; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2004, p. 16; "Verizon Hawaii, Inc. (GTHI)," Federal Communications Commission, <https://www.fcc.gov/verizon-hawaii-inc-gthi>.

³ Decision and Order No. 21696, *In the Matter of the Application of Paradise Mergersub, Inc., GTE Corporation, Verizon Hawaii Inc., Bell Atlantic Communications, Inc., and Verizon Select Services Inc. for Approval of a Merger Transaction and Related Matters.*, No. 04-0140 ("Verizon Decision and Order No. 21696"), <https://files.hawaii.gov/dcca/dca/dno/dno2005/21696.pdf>, p. 20; Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, pp. 50-51.

⁴ As described in **Section III.A**, there is overlap between the corporate and operational timelines.

⁵ Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2003, p. 15; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2004, p. 16. Because the public record does not disclose the date of the beginning of these discussions, I will begin the corporate timeline with the March 12, 2004, disclosure.

⁶ Verizon had 48.8 million access lines, according to its FY2005 Form 10-K. See Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2005, p. 1.

approximately 60 days later on May 21, 2004.⁷ The corporate timeline ended with the closing of the deal approximately 345 days later (on May 2, 2005) when Verizon Hawaii, Inc. became Hawaiian Telecom (“HawaiianTel”), “a stand-alone telecommunications provider.”⁸

3. The operational timeline began before closing, on February 4, 2005, with the buyer’s hiring of BearingPoint to create the necessary back-office systems for a new, stand-alone HawaiianTel.⁹ The operational timeline ended 422 days later on April 1, 2006, when the final cutover to these systems occurred.¹⁰

4. The year between deal signing and deal close provided Verizon and HawaiianTel time to plan the operational details of the divestiture. The critical operational issues revolved around the back-office and information technology software challenges of splitting off integrated assets and establishing a stand-alone entity.¹¹

5. The parties predicted that HawaiianTel would, for a period of approximately 270 days after closing, need Verizon’s continued operational assistance in order to do business.¹² To that end, at closing, Verizon and HawaiianTel entered into a TSA under which Verizon would provide HawaiianTel with, among other things, services, access, maintenance, and support for a number of IT applications as well as billing and customer service support.¹³ 228 days later, in December 2005, the parties realized that they had

⁷ Verizon Decision and Order No. 21696.

⁸ Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 5; “Verizon Hawaii, Inc. (GTHI),” Federal Communications Commission, <https://www.fcc.gov/verizon-hawaii-inc-gthi>.

⁹ Verizon Decision and Order No. 21696, p. 20.

¹⁰ Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, pp. 50-51.

¹¹ As HawaiianTel revealed in its Form S-4 dated January 19, 2006, “[d]uring the transition period, we are putting in place, and making a substantial investment in, a new back-office and IT infrastructure.” See Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 70.

¹² The TSA established an initial transition period of nine months. See Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7.

¹³ Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7.

underestimated the complexity of the software transition, and the TSA was amended to extend the initial 276-day period by another 60 days, to April 1, 2006.¹⁴

2. *Northeast Business (2007)*

6. In 2007, Verizon divested its access lines in Maine, Vermont and New Hampshire, all long-term holdings of Verizon (“Northeast Business”).¹⁵ This divestiture was a lengthy process, taking a total of 757 days between signing of the agreement and the final operational cutover. Of those 757 days, the corporate timeline represented 422 days¹⁶ and the operational timeline represented at least 727 days (from the time cutover planning pursuant to the TSA commenced on February 14, 2007, to the final operational cutover on February 9, 2009).¹⁷

7. The corporate timeline for the Northeast Business divestiture began no later than January 15, 2007,¹⁸ when Verizon’s Northern New England Spinco Inc., and FairPoint Communications, Inc. (“FairPoint”) signed an Agreement and Plan of Merger with regard to the divestment of “approximately 1.5 million access lines in 352 exchanges in Maine, New Hampshire, and Vermont.”¹⁹ The corporate timeline

¹⁴ The amendment to the initial agreement, dated December 15, 2005, extended the transition period for an additional 60 days to April 1, 2006. *See* Hawaiian Telcom Communications, Inc., Hawaiian Telcom, Inc., Hawaiian Telcom Services Company, Inc., Form S-4 Registration Statement, dated January 19, 2006, <https://www.sec.gov/Archives/edgar/data/46216/000119312506008763/ds4.htm>, p. 7.

¹⁵ *See* Bob Varettoni, “Verizon Communications History,” Verizon, September 16, 2016, https://www.verizon.com/about/sites/default/files/Verizon_History_0916.pdf.

¹⁶ The corporate timeline for this divestiture began on January 15, 2007, with the announcement of a deal between Verizon and FairPoint Communications, an established telecommunications provider, and ended on March 31, 2008, with the closing of the deal. *See* Agreement and Plan of Merger by and Among Verizon Communications Inc., Northern New England Spinco Inc., and FairPoint Communications, Inc., January 15, 2007; Joint Application for Approval of the Transfer of Certain Assets by Verizon New England Inc., Bell Atlantic Communications, Inc., NYNEX Long Distance Company, and Verizon Select Services Inc. and Associated Transactions (“Verizon and FairPoint Communications Joint Application for Asset Transfer”); FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 2.

¹⁷ Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-0111/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>; FairPoint Communications, Inc., Form 10-K for the Fiscal Year Ended December 31, 2008, pp. 2-3.

¹⁸ Agreement and Plan of Merger by and Among Verizon Communications Inc., Northern New England Spinco Inc., and FairPoint Communications, Inc., January 15, 2007; Verizon and FairPoint Communications Joint Application for Asset Transfer .

¹⁹ Memorandum Opinion and Order, *In the Matter of Applications Filed for the Transfer of Certain Spectrum Licenses and Section 214 Authorizations in the States of Maine, New Hampshire, and Vermont from Verizon Communications Inc. and Its Subsidiaries to FairPoint Communications, Inc.*, WC Docket No. 07-22, January 9, 2008, p. 3; “Verizon and FairPoint Agree to Merge Verizon’s Wireline Businesses in Maine, New Hampshire

ended with the closing of the deal approximately 422 days later on March 31, 2008.²⁰ The operational timeline largely overlapped with the corporate timeline and began on February 14, 2007 (30 days after the Agreement and Plan of Merger was signed), when the planning for the transition started pursuant to the TSAs and MSAs.²¹

8. The more than a year between deal signing and deal close permitted Verizon and FairPoint ample time to plan the operational details of the divestiture. The critical operational issues revolved around the information technology challenges of splitting off integrated assets and creating new systems to run the assets.²² The parties determined that FairPoint would address this challenge by entering into a TSA with Verizon and an MSA with Capgemini U.S. LLC., which provided services related to the transition, replication, and/or replacement of certain business operations, on January 15, 2007.²³

9. The parties predicted that FairPoint would, for a period of approximately 180 days after closing, need Verizon's continued operational assistance in order to do business.²⁴ To that end, Verizon and FairPoint entered into a TSA under which Verizon would provide FairPoint with, among other services, human resources, regulations, networks database, and benefits delivery.²⁵ 184 days later, in September

and Vermont," Verizon News Archives, January 16, 2007, <https://www.verizon.com/about/news/press-releases/verizon-and-fairpoint-agree-merge-verizons-wireline-businesses-maine-new-hampshire-and-vermont>.

²⁰ FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 2.

²¹ Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>, p. 13 ("Within 30 calendar days following the date hereof [January 15, 2007, also when the Agreement and Plan of Merger was signed], the Cutover Planning Committee shall hold its initial meeting to commence planning and preparation for the Buyers to cease using all Transition Services and thereafter.").

²² FairPoint disclosed that it would build "new systems and processes to replace those used by Verizon to operate and support our network and back office functions in Maine, New Hampshire and Vermont." See FairPoint Communications, Inc., Form 10-K for the Fiscal Year Ended December 31, 2008, p. 2.

²³ FairPoint Communications, Inc., Form 10-Q/A for the Quarterly Period Ended September 30, 2009, p. 89; Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>; Capgemini U.S. LLC and FairPoint Communications, Inc., Master Services Agreement between Capgemini U.S. LLC and FairPoint Communications, Inc.

²⁴ Services provided under transition services agreement were designated for "the projected six month period." (See FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended March 31, 2008, p. 55.)

²⁵ Transition Services Agreement by and Among Verizon Information Technologies LLC, Northern New England Telephone Operations Inc., Enhanced Communications of Northern New England Inc. and FairPoint Communications, Inc., dated January 15, 2007, <https://www.puc.nh.gov/Regulatory/CaseFile/2007/07-011/TESTIMONY/Transition%20Service%20Agreement%20Sch%20A-E%20Exhibit%20SES-4%2003-23-07.pdf>.

2008, the parties realized that they had underestimated the length of the IT transition and extended the TSA services through January 2009.²⁶ Specifically, despite a significant amount of pre-cutover system testing, FairPoint experienced numerous problems with systems and processes that affected “email service, billing, customer call centers, repair service centers, and the order provisioning operations of the Company throughout its Northern New England territory.”²⁷ On February 9, 2009, FairPoint completed the cutover process and began operating its new systems independently from the Verizon systems, 757 days after signing of the agreement.²⁸

3. *14-State Divestiture (2009)*

10. In 2009, Verizon began the divestiture of operations in 13 states that were long-term holdings of Verizon’s corporate predecessor GTE as well as its long-held operations in West Virginia to Frontier Communications Corporation (“Frontier”) in a deal that ultimately took nearly three years to complete (“14-State Divestiture”). This divestiture spanned 1,056 days between signing of the agreement and the final operational cutover. Of those 1,056 days, the corporate timeline represented 415 days²⁹ and the operational timeline represented at least 642 days (from the deal closing on July 1, 2010, to the final operational cutover on April 2, 2012).³⁰

²⁶ FairPoint Communications, Inc., Form 10-Q for the Quarterly Period Ended September 30, 2008, p. 54 (“We expect to continue to require transition services agreement services from Verizon through January 2009, which is beyond the six month period following the closing of the merger, during which we anticipated requiring such services.”). *See also 2009 Annual Report*, State of Maine Public Utilities Commission, February 1, 2010, <https://www.maine.gov/mpuc/sites/maine.gov/mpuc/files/inline-files/AR09-FINAL.pdf>, p. 13.

²⁷ *2009 Annual Report*, State of Maine Public Utilities Commission, February 1, 2010, <https://www.maine.gov/mpuc/sites/maine.gov/mpuc/files/inline-files/AR09-FINAL.pdf>, p. 11.

²⁸ FairPoint Communications, Inc., Form 10-K for the Fiscal Year Ended December 31, 2008, p. 3.

²⁹ The corporate timeline for the Frontier divestiture began no later than May 13, 2009, when the parties signed an agreement and ended with the closing of the deal on July 1, 2010. *See FCC Memorandum Opinion and Order, In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 4; Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2010, Note 3; “Verizon Completes Spinoff of Local Exchange Businesses and Related Landline Activities in 14 States,” Verizon News Archives, July 1, 2010, <https://www.verizon.com/about/news/press-releases/verizon-completes-spinoff-local-exchange-businesses-and-related-landline-activities-14-states>.

³⁰ Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.

11. The corporate timeline for the 14-State Divestiture began no later than May 13, 2009, when Frontier signed an agreement to acquire Verizon's Wireless Operations in 14 states for \$8.5 billion.³¹ The corporate timeline ended on July 1, 2010, 415 days later, when the deal closed and Verizon spun off a subsidiary called New Communications Holdings Inc. (the "Midwest Spinco") that merged with Frontier pursuant to a definitive agreement.³²

12. The public record provides no ascertainable date for the beginning of the operational timeline. Although planning for the cutover undoubtedly began earlier, the observable operational timeline ran from the closing of the deal on July 1, 2010, until Frontier completed the integration of operations to its own systems on April 2, 2012, 642 days later. Over this nearly two-year period, underlying operations support for the former GTE operations in 13 states were provided through a replica version of Verizon's software until they were migrated to Frontier's own systems.³³

13. In October 2011, all acquired operations in Indiana, Michigan, North Carolina and South Carolina migrated to Frontier's operating systems and the acquired operations in 13 states were incorporated into Frontier's financial and human resources systems.³⁴ Frontier anticipated commencing the systems conversion in the remaining states in March 2012.³⁵ Finally, in April 2012, the acquired operations in Arizona, California, Idaho, Illinois, Nevada, Ohio, Oregon, Washington and Wisconsin were transitioned to Frontier's legacy operating systems.³⁶ The lines in West Virginia, approximately 13 percent of the total

³¹ FCC Memorandum Opinion and Order, *In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 4.

³² Verizon Communications Inc., Form 10-K for the Fiscal Year Ended December 31, 2010, Note 3; "Verizon Completes Spinoff of Local Exchange Businesses and Related Landline Activities in 14 States," Verizon News Archives, July 1, 2010, <https://www.verizon.com/about/news/press-releases/verizon-completes-spinoff-local-exchange-businesses-and-related-landline-activities-14-states>.

³³ Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>; FCC Memorandum Opinion and Order, *In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 12.

³⁴ Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.

³⁵ Frontier Communications Corporation, Form 10-K for the Year Ended December 31, 2012, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0000020520/b7334365-f330-4e9d-8f5b-850623fd18d8.pdf>, p. 2.

³⁶ Frontier Communications, Customers Benefit as Frontier Communications Completes 14-State Systems Conversion, dated April 2, 2012, <https://www.sec.gov/Archives/edgar/data/20520/000002052012000026/conversionpr.htm>.

involved in the transaction, were migrated from Verizon's systems to Frontier's systems on or about the closing date.³⁷

³⁷ Of the 4.8 million access lines included in the transaction, 600,000 lines were in West Virginia. (See "FCC Approves Historic Deal Between Verizon and Frontier, All Necessary Approvals Now Granted," telecompetitor, May 21, 2010, <https://www.telecompetitor.com/fcc-approves-historic-deal-between-verizon-and-frontier-all-necessary-approvals-now-granted/>; FCC Memorandum Opinion and Order, *In the Matter of Applications Filed by Frontier Communications Corporation and Verizon Communications Inc. for Assignment or Transfer of Control*, WC Docket No. 09-95, May 21, 2010, p. 15.) While the parties were able to cutover the sole legacy Bell Atlantic jurisdiction (West Virginia) on or about the closing date, the cutover for the remaining GTE properties required a lengthy transition process.

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC.,

and

BYTEDANCE LTD.,

Petitioners,

v.

No. 24-1113

MERRICK B. GARLAND, in his official
Capacity as United States Attorney
General,
Respondent.

DECLARATION OF CHRISTOPHER P. SIMKINS

I, Christopher P. Simkins, under penalty of perjury, hereby declare as follows:

BACKGROUND

1. I am the CEO and Founder of Laconia Law & Consulting and have held that position since 2008. I am also the CEO and Co-Founder of Shouldrs, Inc. In addition, I serve as a Director on the Board of Directors for Zetec, Inc. I received my B.A. and J.D. from Brigham Young University in 1993 and 1997 respectively. I have attached a true and correct copy of my curriculum vitae to this declaration.

2. For the past 20 years, I have worked at the intersection of U.S. national security and business. From 2004 to 2007, I served in the U.S. Department of Justice (“DOJ”). I started as a prosecutor and investigator in DOJ’s Counterespionage Section. My primary areas of focus were China and investigations of media leaks of classified programs. I subsequently led DOJ’s

participation on the Committee on Foreign Investment in the United States (“CFIUS”). I was promoted to Senior Counsel within DOJ’s Criminal Division and then National Security Division, which was created during my tenure. I was responsible for coordinating DOJ’s (including FBI’s) participation in the CFIUS process and directly advised the Attorney General and Deputy Attorney General on CFIUS matters.

3. As DOJ’s lead on CFIUS, I reviewed over 200 transactions. I was the lead negotiator on behalf of CFIUS for most of the prominent transactions reviewed from 2004-2007. I authored multiple requests to the President to exercise executive authority to block transactions. I was the primary architect and drafter of multiple complex national security mitigation agreements and worked with the FBI and other CFIUS agencies such as the Department of Defense, the Department of Homeland Security, and Intelligence Community agencies to assess national risks and to develop mitigation strategies. Most of the complex CFIUS matters I handled involved transactions with technology companies, including in sectors such as telecommunications, cloud computing, semiconductor design, data center technology, and computer software. I led CFIUS mitigation negotiations that were among the first to include complex physical and logical access restrictions to technology platforms and reliance upon source code review as means of discovering and deterring attacks by nation-states.

4. Since 2008, I have been a national security consultant and lawyer and simultaneously have started multiple companies, including Corsha, Inc., a successful technology company that offers a patented cybersecurity solution for machine-to-machine network traffic that I was involved in designing and developing. From 2011 to 2017, I was the CEO and Co-Founder of Chain Security, LLC, a professional services firm. Our clients were primarily technology companies who were selling computing equipment and software, including

cybersecurity software, to the U.S. Government and U.S. critical infrastructure. Our customers typically hired us to help analyze and solve concerns raised by government customers concerning technology supply chains as well as research, development, and production being performed outside the U.S., most often in China. As a consultant, I advise large corporations, technology companies, and defense contractors on national security matters, including CFIUS transactions, as well as operations and processes required to protect sensitive information. I currently serve as a technology and security advisor for a biotech company, and I am also currently an advisor to two different companies in the national security space where one of my roles is to assess commercial technology platforms for repurposing as national security platforms. I also serve as a consultant and expert to law firms handling CFIUS transactions. I have led efforts to analyze national security vulnerabilities and to put in place operational and technical mitigation plans that were presented to government customers, including tracing the origins of software and hardware components and maintaining secure chains of custody for software. I remain abreast of current CFIUS trends and approaches to mitigation as well as how U.S. Government agencies with defense, intelligence, and law enforcement responsibilities assess risks associated with the security of data and information systems, particularly with respect to China. I have been a testifying expert in CFIUS-related litigation. A copy of my curriculum vitae is attached hereto as Appendix 1.

SUMMARY OF DECLARATION

5. Through their counsel, I have been retained by Petitioners TikTok Inc. and ByteDance Ltd. (“Petitioners”)¹ to analyze the draft National Security Agreement, dated August

¹ References to ByteDance are to the corporate group as opposed to any particular corporate entity. However, such references exclude TikTok U.S. Data Security Inc. (“TTUSDS”), as discussed *infra* paras. 39, 46-50, 53.

23, 2022, between these parties and CFIUS (“NSA”), and to offer an opinion on whether the NSA as drafted would mitigate the national security concerns expressed by sponsors of the Protecting Americans From Foreign Adversary Controlled Applications Act (the “Act”) which coincide with the rationale expressed by CFIUS during its TikTok review.

6. Throughout this Declaration, I will use the term “TikTok U.S. App” or simply the “App” to mean collectively the TikTok mobile app and the web-based version of TikTok that specifically are used by a “TikTok U.S. User.”² A “TikTok U.S. User” or “User” is a person using the App who is (i) in the U.S., or (ii) outside the U.S. but is identifiable as a U.S. person.³ I will use the term “TikTok U.S. Platform” or simply the “Platform” to mean the platform components (as explained more fully below) that specifically support the TikTok U.S. App.⁴

7. The U.S. Government, including Congress and CFIUS, use a widely adopted model for assessing national security risks. The risk model has multiple components—threat, vulnerability, and consequences. Using an analytic approach to each component enables decision makers to understand what mitigation may be required to lower national security risk to acceptable levels.

8. CFIUS and Petitioners engaged in protracted and detailed mitigation negotiations over the course of nearly two years, culminating in the NSA. I have reviewed the NSA. Using the risk model, my professional opinion is that if implemented as written, the NSA would effectively mitigate the U.S. national security risks associated with Petitioners owning and deploying the TikTok U.S. App and TikTok U.S. Platform.

² See NSA Sec. 1.33.

³ See NSA Sec. 1.35.

⁴ See NSA Sec. 1.34.

9. I have organized this Declaration into the following sections, with references to the corresponding paragraphs:

- A. METHODOLOGY (paras. 10-29), which includes these subsections:
 - i. Overview of the Risk Model (paras. 11-17)
 - ii. Threat (para. 18)
 - iii. Vulnerability/Consequences (paras. 19-22)
 - iv. The Role of Mitigation (paras. 23-29)
- B. ANALYSIS (paras. 30-104), which includes these subsections:
 - i. History of Negotiations (paras. 32-37)
 - ii. Key Elements of the NSA (paras. 38-75)
 - iii. Caveats and Assumptions (paras. 76-80)
 - iv. Analysis of the NSA (paras. 81-104)
- C. CONCLUSIONS (paras. 105-107)

METHODOLOGY

10. To assess the NSA, I will use the established risk-based methodology that is well-known and well-accepted across the government's national security community. First, I will frame the model's importance in national security decision making and summarize how the model works. I will then discuss in more depth each of the components or parameters that feed into the risk model. I will then discuss the role of mitigation in addressing national security risk.

Overview of the Risk Model

11. It is important to understand the reasons for using a model for analyzing national security risk, rather than falling back on broad or vague national "interests" tests when making national security decisions. By relying on an analytic model with specific parameters, the U.S.

Government is empowered to make better decisions about when to take action to protect national security interests and what actions to take. The model ensures that Congress, CFIUS, and other government decision makers are more rigorous in assessing which specific mitigation mechanisms are needed to protect national security, how those mechanisms should be implemented and by whom, and how to measure their effectiveness. The model is intended to blunt the temptation to substitute political decisions or “gut feelings” for analysis in situations where, either by long-standing consensus or as mandated by law, a more precise, thoughtful, and thorough national security determination is required.

12. U.S. Government agencies use this risk model when assessing cybersecurity risks and other national security risks to networks, data, privacy, and information systems.⁵ For example, as recently as March 2024, the Government Accountability Office relied on this risk model when advising Congress on cybersecurity risks to critical infrastructure systems.⁶ In 2018, Congress codified this risk model in the statute that governs CFIUS, requiring CFIUS to use the model when deciding whether to allow, block, or mitigate transactions under review.⁷ CFIUS has likewise codified this risk model in its regulations.⁸

⁵ See, e.g., Nat’l Counterintelligence and Sec. Ctr., Off. of Dir. of Nat’l Intel., *Framework for Assessing Risks* (April 2021), https://www.dni.gov/files/NCSC/documents/supplychain/Framework_for_Assessing_Risks_-_FINAL_Doc.pdf [hereinafter “ODNI Framework”]; Nat’l Inst. of Standards & Tech., Dep’t of Com., NIST Special Pub. 800-30 Rev. 1, *Guide for Conducting Risk Assessments* (Sept. 2012), <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>; Dep’t of Homeland Sec., *DHS Risk Lexicon* (Sept. 2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf> [hereinafter “DHS Lexicon”].

⁶ See U.S. Gov’t Accountability Off., *Cybersecurity: Improvements Needed in Addressing Risks to Operational Technology* (Mar. 2024), <https://www.gao.gov/assets/gao-24-106576.pdf>.

⁷ See Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. 115-232, 132 Stat. 2174 (2018) (codified at 50 U.S.C. § 4565).

⁸ See 31 C.F.R. § 800.102 (Risk-based analysis).

13. In the lexicon of this model, “risk” is a term of art. The simplified formula for risk is as follows: $\text{Risk} = \text{Threat} * \text{Vulnerability/Consequences}$. Because each of these elements – threat and vulnerability/consequences– are qualitative rather than quantitative, the formula is obviously not intended to be mathematical. Instead, it represents a qualitative combination of each element to make a holistic determination about national security interests.

14. When conducting an analysis using the model, a decision maker or analyst considers each of the elements independently using data that is specific to the element. Each element is then typically scored as low, medium, or high. The elements are then combined or “averaged” to produce an overall risk that is either low, medium, or high. For example, in a given national security context, such as an acquisition of a U.S. company by a non-U.S. buyer, the model could indicate that the THREAT is LOW and the VULNERABILITY/CONSEQUENCES is HIGH, leading to a conclusion that the overall RISK to national security for the transaction is HIGH. Similarly, e.g., the model could indicate that the THREAT is HIGH, but the VULNERABILITY/ CONSEQUENCES are LOW, giving the transaction an overall risk of LOW.

15. Again, the formula is ultimately qualitative, so it is not as simple as saying, e.g., two LOWs and a HIGH average out to a MEDIUM. Some judgment and weighting are required, depending on the context. The qualitative risk scoring guides the analysis and suggests roughly the overall risk outcome.

16. In my experience in the CFIUS context, when the model indicates that the national security risk for a transaction is HIGH, CFIUS typically either (i) has demanded that the parties agree to mitigation or (ii), in cases where mitigation was not sufficient or if the parties would not agree to CFIUS’s demands, has recommended that the President exercise his authority

to block the transaction or requested the parties to abandon the transaction. For transactions that are rated as a MEDIUM risk, CFIUS has typically required some level of mitigation, but has rarely blocked such transactions. Transactions with LOW risk are typically approved without further action.

17. When assessing any of the model's components, U.S. Government decision makers typically rely on a mix of publicly available information, unclassified but confidential government information, and classified information. Congress and CFIUS can draw on reporting from the U.S. intelligence, defense, and law enforcement communities, particularly for threat information, as well as on expertise across the government for sensitive information about threats, vulnerabilities, and consequences. Parties to a transaction, such as the Petitioners, are also very important sources of information, particularly related to vulnerabilities. Government agencies also use a review of open-source information to understand technologies, industry dynamics, and customer use cases.

Threat

18. Under the lexicon of the risk model, "threat" focuses on an assessment of the foreign or non-U.S. actors in the context. For example, the threat analysis here would be focused on ByteDance and, because it is indirectly wholly owned by ByteDance Ltd., TikTok Inc. The specific question when assessing a threat is whether the foreign person at issue has (a) an intent and (b) a capability to take action that would impair U.S. national security.⁹ As discussed below, I assume for purposes of this Declaration, that the U.S. Government will consider the Chinese

⁹ See, e.g., 31 C.F.R. § 800.102(a) (CFIUS definition of "threat"); see also ODNI Framework, *supra* note 5, at 2 ("From the threat perspective, an understanding of the adversary's intentions and capabilities is vital. Key to this is using the latest threat information to determine if specific and credible evidence suggests an item or service might be targeted by adversaries.").

government and most if not all Chinese companies as posing a HIGH threat to U.S. national security interests.

Vulnerability/Consequences

19. The “vulnerability” and consequences analyses are focused on the U.S. company, U.S. person, or U.S.-based assets in the transaction. The analysis can consider an entire U.S. business or just U.S.-based assets, data, or operations in the business.

20. The vulnerability analysis for the current context would be focused on the TikTok U.S. App and the TikTok U.S. Platform. The specific question when assessing a vulnerability is whether the U.S. company, person, or assets could be exploited by the foreign person (i.e., the foreign “threat” actor) to hurt or impair U.S. national security.¹⁰

21. Sponsors of the Act identified two U.S. interests that could be harmed by the Petitioners through their control of the TikTok U.S. App and the TikTok U.S. Platform.¹¹ The first is the data about U.S. users or subgroups of users that is gathered by or stored on the TikTok U.S. Platform as a result of using the TikTok U.S. App. The data could include personal identifying information, financial information, geolocation, social connections, and patterns of

¹⁰ See, e.g., 31 C.F.R. § 800.102(b) (CFIUS definition of “vulnerability”); see also DHS Lexicon, *supra* note 5, at 38 (“physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard”).

¹¹ While I have limited my discussion in this Declaration to the two asserted vulnerabilities that apparently motivated the sponsors of the Act, as part of my analysis I considered an expanded array of relevant national security vulnerabilities, including those cited by CFIUS. See, e.g., Exec. Order No. 14083, Sec. 3(c)(i), 87 Fed. Reg. 57369, 57372-73 (Sept. 15, 2022); Letter from Thomas P. Feddo, Assistant Secretary Investment Security, U.S. Dept. of Treasury (on behalf of CFIUS) to David N. Fagan and Michael E. Leiter (counsel for ByteDance and TikTok) 3 (Jul. 30, 2020) (CFIUS referral to the President). My opinion that the NSA would effectively mitigate national security risks includes mitigating the full array of vulnerabilities I considered that could possibly be associated with the TikTok U.S. App and the TikTok U.S. Platform.

behavior. Whether standing alone or combined with other compromised data sets, compromised user data could be used for “the surveillance, tracing, tracking, and targeting of individuals or groups of individuals,” particularly in light of recent advancements in artificial intelligence and data science.¹² The second interest identified by congressional sponsors of the Act is that the content on the TikTok U.S. Platform could be manipulated to serve the interests of the Chinese government through spreading pro-Chinese propaganda, censoring anti-Chinese content, or promoting content intended to incite disunity and foment hate in the U.S. on divisive issues.

22. The “consequences” (sometimes called “impact”) assessment is closely related to the vulnerability assessment and is often included as an element of vulnerability. The consequences assessment focuses on the specific national security interests at stake or affected by the U.S. company, person, or asset. It seeks to characterize how much damage would be caused to national security if a vulnerability is exploited.

The Role of Mitigation

23. The role of mitigation is to reduce specific elements of the risk model such that the overall national security risk level drops to an acceptable level, typically LOW or MEDIUM. To accomplish this, mitigation must be specifically tuned to the elements of threat and vulnerability, including consequences.

24. Mitigation is typically accomplished by imposing a legal obligation on the parties in a particular national security context to take action to mitigate the risk. These legal obligations typically take the form of an agreement with the U.S. Government, or they may include unilateral action taken by private parties. In the context of business operations and

¹² Exec. Order 14083, Sec. 3(c)(i), 87 Fed. Reg. at 57372-73.

mergers and acquisitions, the mitigation obligations can be required of a foreign actor, a U.S. actor, or both. The NSA is an example of such a mitigation contract.

25. The U.S. Government has a long history of favoring mitigation to reduce national security risks. CFIUS is a prime, but not exclusive, example of a government entity engaging in mitigation to reduce risk. The Federal Communications Commission (“FCC”), in conjunction with the interagency group “Team Telecom,”¹³ adopts mitigation agreements similar to those imposed by CFIUS as a condition of granting Section 214 licenses to non-U.S. applicants for the provision of international telecommunications services to or from the United States. The U.S. Department of Defense as well as Intelligence Community agencies frequently enter into mitigation agreements to address foreign ownership, control, and influence by foreign persons over U.S. companies and will also enter into agreements or require unilateral action to reduce risk in technology supply chains.

26. CFIUS has been reluctant to use mitigation to lower national security risk when the mitigation depends on an untrusted foreign company to faithfully implement the mitigation terms. CFIUS has reasoned that, e.g., it cannot trust a Chinese company to comply with contractual mitigation commitments if the Chinese government at some point demands that the company take action against U.S. national security interests. This is the reason many China-related transactions have been turned away by CFIUS in recent years, when similar transactions deriving from other high-threat countries have been cleared subject to mitigation.

27. The exception to this pattern is when CFIUS has been able to rely on a trusted third-party U.S. company as the primary mechanism for ensuring compliance with mitigation, even in China-related transactions. In such cases CFIUS has been able to get comfortable with

¹³ See Exec. Order 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020).

entering into mitigation agreements similar to the NSA. Under the rubric of the risk model, the reliance on a trusted third party helps reduce the foreign party's access to U.S. national security assets and thereby effectively reduces the ability of the foreign party to exploit vulnerabilities.

28. A public example of this is the CFIUS approval in 2018 of the proposed acquisition of Genworth Financial, a U.S. mortgage insurance provider, by China Oceanwide Holdings. CFIUS's approval was conditioned on the use of "a U.S.-based, third-party service provider to manage and protect the personal data of Genworth's U.S. policyholders" after the transaction closed.¹⁴ Another public example is Lenovo's acquisition of IBM's PC Division in 2005 and its subsequent acquisition of IBM's X86 server business in 2014.¹⁵ CFIUS approved both transactions subject to mitigation agreements that required IBM to continue playing a primary role in servicing the computing equipment for years after the transaction closed, despite no longer owning the sold assets. CFIUS was able to rely on IBM's bona fides to ensure that the key technical and process-related terms of the mitigation were faithfully and effectively implemented, without having to rely on Lenovo, which at the time was a Chinese company with Chinese government ownership.

29. In addition to using a trusted U.S. third party to lower the vulnerability level, mitigation agreements used by not only CFIUS but other government agencies have relied on a

¹⁴ See *Genworth Financial Announces Second Quarter 2018 Results*, Genworth (Jul. 31, 2018) <https://investor.genworth.com/sec-filings/all-sec-filings/content/0001193125-18-233445/d610764dex991.htm>.

¹⁵ See, e.g., Patrick Moorhead, *IBM-Lenovo Server Agreement Basically a Done Deal*, Forbes (Aug. 26, 2014) <https://www.forbes.com/sites/patrickmoorhead/2014/08/26/ibm-lenovo-server-agreement-basically-a-done-deal/?sh=aa570a24bbc7>; *Committee on Foreign Investment in U.S. Completes Review of Lenovo-IBM Deal*, Lenovo (Mar. 9, 2005) <https://news.lenovo.com/pressroom/press-releases/committee-on-foreign-investment-in-u-s-completes-review-of-lenovo-ibm-deal/>.

number of well-accepted mitigation principles, primarily aimed at reducing vulnerabilities. They include (i) technical and operational processes that eliminate or materially reduce access to products and services, with a goal of reducing the level of access available to a foreign “threat” actor to exploit vulnerabilities; (ii) mechanisms for high visibility and accountability through inspections, auditing, and monitoring, with the goal of deterring a foreign “threat” actor from taking adverse action that would be discovered and could lead to significant criminal penalties or unilateral action by U.S. law enforcement, defense, and/or intelligence agencies; (iii) automatic and in some cases liquidated damages provisions and other enforcement and penalty mechanisms for non-compliance, with the goal of deterring exploitation with a threat of significant monetary penalties; and (iv) provisions allowing for CFIUS to reopen reviews or unilaterally initiate stoppages or even divestment for material non-compliance, which preserves CFIUS’s power to take additional action to protect national security for the entire term of a mitigation agreement.

ANALYSIS

30. The purpose of this Declaration is to analyze the NSA as written and offer an opinion, based on my professional experience, as to whether it is sufficient to mitigate national security risk to a level that should be acceptable to Congress and CFIUS.

31. I believe it is important to contextualize the NSA. Based on my experience negotiating other such agreements, the NSA was likely the result of thousands of collective hours of work between CFIUS, the Petitioners, and their advisors to arrive at the best possible solution to address national security risk in the context of the TikTok U.S. App and the TikTok U.S. Platform. I therefore will summarize the history of negotiations surrounding the NSA. I will then provide an overview description of the key terms of the NSA as well as an explanation of important caveats and assumptions that are relevant to my analysis. I will then analyze the terms

of the NSA itself using the risk model I have described above and will draw conclusions about the effectiveness of the NSA's terms to mitigate national security risk.

History of Negotiations

32. Petitioners formally filed a voluntary notice with CFIUS on May 27, 2020. A first period of engagement resulted in CFIUS referring the matter to President Trump on July 30, 2020, and President Trump issuing a divestment order on August 14, 2020.

33. I understand that Petitioners and the U.S. Government agreed to an abeyance of the litigation Petitioners brought challenging the divestment order so they could engage in negotiations to determine whether mitigation was possible.

34. After exchanging terms sheets, Petitioners provided CFIUS with a first draft of the NSA on January 4, 2021. From January 2021 through August 2022, Petitioners and CFIUS engaged in active negotiations regarding the terms of the NSA. Based on the CFIUS record, at least 23 sets of revisions to the NSA were exchanged between the parties. In that time period, CFIUS heavily redlined all or a portion of the NSA eight different times. Many of CFIUS's revisions or comments reflect that the Committee and its agencies very actively tried to understand the TikTok U.S. App and platform and how they would operate at a technical level. The substantive provisions of the NSA that CFIUS commented on or revised ranged from corporate governance, U.S. control of TikTok U.S. Data Security Inc. ("TTUSDS"), hiring by TTUSDS, the role of the Trusted Technology Partner,¹⁶ use of technical vendors and contractors, mechanisms for source code review, chain of custody for reviewed code, storage and protection of "Protected Data," monitoring, auditing, and enforcement. Petitioners' responses appear to incorporate or accept with some revision the vast majority of revisions proposed by CFIUS.

¹⁶ As discussed *infra* paras. 54-56.

35. In addition to written redline exchanges, the CFIUS record indicates that between January 2021 and August 2022, there were at least 14 meetings or calls between CFIUS and Petitioners to discuss NSA terms. The meetings included at least nine written presentations by Petitioners to CFIUS about the NSA mitigation mechanisms and the status of implementation. In addition to meetings and presentations, there were at least 15 additional email exchanges where CFIUS posed questions related to Petitioners' operations and the NSA terms, which emails were followed by written responses by Petitioners.

36. In short, CFIUS and Petitioners had a protracted, detailed, and productive negotiation over nearly two years that led to the version of the NSA at issue here.

37. The final working draft of the NSA was delivered by Petitioners to CFIUS on August 23, 2022. Including its annexes, the NSA is 103 pages long and is the most sophisticated and thorough mitigation agreement I have reviewed in my 20 years of working on national security agreements, including my time as a member of CFIUS and in my current legal and consulting roles advising companies in their negotiations with CFIUS as well as with the Department of Defense and the Intelligence Community.

Key Elements of the NSA

38. The NSA is lengthy and has a significant amount of detail about the overarching mitigation mechanisms. I will not recount all of the details, but to inform my analysis of the terms, I provide here an overview description of the key terms of the NSA that I believe are most relevant to my analysis and conclusions. I will define a few key terms that are important to understanding the NSA. I am using definitions in a more colloquial way than the precise

contractual language in the NSA. The precise definitions of these terms will of course still be informed by the NSA itself.¹⁷

39. The NSA requires the creation of a new entity called TTUSDS. It is to be a U.S. corporation and a wholly owned subsidiary of TikTok Inc. The role of TTUSDS is critical to the NSA.¹⁸

40. Non-public personal information about TikTok U.S. Users, whether it is provided to the App by the User or gathered from use of the App, is defined as “Protected Data.”¹⁹ It is this Protected Data that is central to one of the two national security risks raised by sponsors of the Act—i.e., intelligence collection. The App and Platform contain other information, such as user content, that is meant to be shared as well as information from other platforms or data sets that is non-confidential such as news and advertisements, all of which is considered to be publicly available and is defined as “Public Data” in the NSA.²⁰

41. The Platform includes various layers of software, including software referred to as the “Recommendation Engine,” which continuously learns from User behavior as well as input from TikTok Inc. to recommend content to TikTok U.S. Users.²¹ This Recommendation Engine is central to the second national security risk raised by sponsors of the Act—i.e., propaganda.

42. When software developers or engineers write computer software, they use words and phrases that describe the logic and commands of the software. There are different coding

¹⁷ I understand that Petitioners may have voluntarily started implementing some of the NSA’s terms. In this Declaration, I will discuss the NSA as if it remains completely prospective.

¹⁸ See NSA Sec. 2.1.

¹⁹ See NSA Sec. 1.22.

²⁰ See NSA Sec. 1.23.

²¹ See NSA Sec. 1.24.

languages that have different ways of phrasing commands and different syntax, but ultimately all coding languages are readable to a human. This human-readable set of commands is called “Source Code.”²² A trained engineer who understands the general function of software and who knows the particular coding language that was used should be able to read Source Code, understand what the software will do and how it will operate, and spot anomalies and vulnerabilities. There are also automated tools available that can read Source Code to ensure integrity and spot vulnerabilities. Source Code reviewers often use these automated tools to assist with manual reviews.

43. To deploy software to a machine or a computer and make it work as an application, Source Code must be converted from words and phrases to “binary” code, which consists of 1s and 0s. This conversion is done through feeding Source Code into a specialized set of applications in a process that is called a “Build.” The output of a Build process that has converted Source Code into a machine-executable application consisting of 1s and 0s is called “Executable Code” (sometimes also called “Object Code” or “Binary”).²³ Humans cannot read or understand Executable Code. There are some specialized applications that can check the integrity of Executable Code and can monitor its behavior when running as a software application. However, identifying vulnerabilities or malicious code is much easier during a Source Code review than when testing Executable Code.

44. During a Build process, the final software can consist of proprietary Source Code developed by a company as well as third party code that may be incorporated into the software. Third party code can be integrated either as Source Code or may be licensed or acquired only in

²² See NSA Sec. 1.28.

²³ See NSA Sec. 1.12.

Binary form. A Build process can combine third-party Executable Code with proprietary Source Code to make a unified software application in a single final Executable form.

45. The App and the Platform are largely composed of software developed by ByteDance and its affiliates. The software is developed as Source Code, which is then run through a Build process to create Executable Code. The Executable Code for the App is published to app stores (e.g., Apple and Google) or loaded onto the TikTok website. The Executable Code for the Platform is deployed to cloud infrastructure, servers, networks, gateways, and databases in order to operate the Platform. The key functionality of the Platform is embedded in software, although that software runs on some physical infrastructure. The manner in which the App and the Platform operates as software depends on both the commands and features in the Code as well as how the App and the Platform are configured when they are installed on phones, computers, cloud infrastructure, servers, networks, and databases.

46. Under the NSA, the overall function of the newly created TTUSDS is to have primary responsibility for the security of the App and the Platform and for the protection of Protected Data. The NSA contains key provisions that directly affect the governance and control of TTUSDS and the access Petitioners have to TTUSDS and the App, the Platform, and Protected Data.²⁴

47. The NSA requires Petitioners to relinquish both governance control and operational control over TTUSDS.²⁵ TTUSDS's Board of Directors will consist of three Security Directors who are U.S. citizens residing in the U.S. and who have had no previous

²⁴ See NSA Sec. 2.4.

²⁵ See NSA Sec. 2.7.

affiliation with Petitioners and who must be approved by the U.S. Government.²⁶ One of the three directors will serve as Chair. There may be other members and observers on the Board, but they can only be persons associated with TTUSDS. No representative of Petitioners can attend or participate with the TTUSDS Board unless the U.S. Government grants express approval. The exception is that TTUSDS will not be able to take certain extraordinary actions without consulting Petitioners, such as selling TTUSDS's assets or filing for bankruptcy. This allowance of Petitioners to have a say in extraordinary action is a standard provision in mitigation agreements, both with CFIUS and when the Department of Defense is mitigating foreign ownership, control, or influence of foreign-owned U.S. companies that perform classified work.

48. The management of TTUSDS will be appointed by the TTUSDS Board, and the key management personnel must all be U.S. citizens with no prior affiliation with Petitioners.²⁷ The only involvement from Petitioners is that TikTok Inc. must be consulted in setting the compensation for TTUSDS's key management personnel.²⁸

49. The NSA also requires a change in the Board of TikTok Inc. The Board will have five members—two representing ByteDance; two outside directors who have had no prior affiliation with Petitioners and who are citizens of the U.S. or one of the “Five Eyes” countries (i.e., Canada, U.K., Australia, and New Zealand); and the Chair of TTUSDS.²⁹ TikTok Inc. must have a Compliance Officer, and TTUSDS must have a Security Officer, who are U.S.

²⁶ See NSA Secs. 3.1-3.2.

²⁷ See NSA Sec. 5.1.

²⁸ See NSA Sec. 3.11(3).

²⁹ See NSA Sec. 4.1.

citizens to be liaisons with TTUSDS as well as with the U.S. Government on compliance and security matters.³⁰

50. Operationally, TTUSDS must be completely separated from Petitioners, with no sharing of locations, systems, networks, or personnel.³¹ TTUSDS will have full autonomy, subject to oversight by the Security Directors and Third-Party Monitor, as described below, over its employees and vendors, with no input or involvement from Petitioners.³²

51. The NSA allows TikTok Inc. to continue managing the business strategy in the U.S. for the App and the Platform and to coordinate that strategy with the rest of the world, which includes identifying new features, gathering customer feedback in the U.S., coordinating with advertisers, and managing certain legal, compliance, and safety matters.³³

52. The Source Code for the App and the Platform will continue to be written primarily by ByteDance, presumably in China.

53. The primary thrust of the NSA is that it sets up key technical and operational security provisions that govern use of the App and the Platform, as well as access to and storage of Protected Data, and places responsibility for all of those activities exclusively in TTUSDS. The NSA refers to these as “CFIUS Functions.” They include: (i) storage and protection of Protected Data, (ii) review and inspection of all Source Code for the App and the Platform prior to the Build process, (iii) actual deployment in the U.S. of all Executable Code for the App and the Platform, (iv) all business and compliance functions that may require access to Protected

³⁰ See NSA Secs. 6.2, 6.3.

³¹ See NSA Secs. 2.2, 2.5, 2.6, 2.7, 12.1(3).

³² See NSA Secs. 13.1-13.7.

³³ See NSA Sec. 4.2.

Data, (v) review and control over the performance of the Recommendation Engine, and (vi) overall compliance with the NSA.³⁴ The NSA requires Petitioners to grant to TTUSDS all of the rights and licenses to the App and the Platform necessary to use them in the U.S.

54. A critical element in the NSA is the appointment of a Trusted Technology Partner (“TTP”) to support TTUSDS in all of these “CFIUS Functions.”³⁵ The U.S. Government must approve the appointment of the TTP. The NSA identifies Oracle, Inc., a publicly traded U.S. company, as the initial TTP. Oracle may be replaced by another approved third-party vendor if needed.³⁶

55. The NSA requires that Petitioners and TTUSDS enter into a master services agreement with Oracle to implement the NSA.³⁷ While Petitioners are responsible for funding the efforts by Oracle, Oracle works solely under the direction of TTUSDS, and its fiduciary obligations are to TTUSDS and the U.S. Government, not to Petitioners. For all the work related to the NSA, Oracle is required to follow the same hiring parameters that govern TTUSDS—i.e., using only individuals who do not work for or have any other affiliation with Petitioners, and with constraints on the hiring of citizens of certain countries, including China.³⁸

56. Oracle’s role is central to the entire mitigation mechanism under the NSA. Oracle will be charged with carrying out the technical aspects of TTUSDS’s obligations to secure the

³⁴ See NSA Sec. 2.4.

³⁵ See NSA Secs. 1.37, 2.4, 2.5.

³⁶ See NSA Sec. 1.37.

³⁷ See NSA Sec. 8.2.

³⁸ See NSA Secs. 1.4, 5.3, 8.2.

App, the Platform, and the Protected Data.³⁹ Oracle will work with other U.S.-based third-party vendors who will play additional roles for TTUSDS, as described below.

57. The NSA's technical mitigation scheme can be understood by examining the process governing the software for the App and the Platform. After ByteDance writes the Source Code for both the App and the Platform (including the Recommendation Engine), it will deliver the Source Code to a facility in the U.S. that the NSA calls a "Dedicated Transparency Center."⁴⁰ This is essentially a computer environment whose sole purpose is to hold the Source Code and make it available to TTUSDS and Oracle. There may be more than one Dedicated Transparency Center, but each one must have an exact copy of any Source Code placed in any other Center (i.e., they are mirrored). ByteDance will be able to push Source Code to the Dedicated Transparency Centers but cannot "pull" any data nor have any other access to the Dedicated Transparency Centers.⁴¹

58. The Dedicated Transparency Centers must be located only in the U.S. or in one of the "Five Eyes" countries.⁴² There must always be a Dedicated Transparency Center located within Oracle's own proprietary secure cloud environment, which I will refer to as the "Secure Oracle Cloud."⁴³

59. When ByteDance delivers Source Code to the Dedicated Transparency Centers, it must also deliver a "software bill of materials" or "SBOM" along with each tranche of Source

³⁹ See NSA Sec. 8.2.

⁴⁰ See NSA Secs. 1.10, 9.2.

⁴¹ See NSA Secs. 9.1, 9.3.

⁴² See NSA Sec. 9.1.

⁴³ See NSA Sec. 9.4; *see also id.* Sec. 8.4.

Code that is lodged.⁴⁴ An SBOM is a detailed list or description of all the components in the Source Code and their sources (e.g., written by ByteDance, licenses from a third party, or open source), which can include individualized Source Code modules for particular features as well as any third-party Source Code or Executable Code.

60. When ByteDance delivers Source Code and an accompanying SBOM, it must electronically sign both of them.⁴⁵ Electronic signatures are a technical method of fingerprinting electronic information or code. There are various methods of doing it, but the essential point is that once code is signed, it is very hard to replicate or spoof the signature. It is a way of uniquely identifying a particular copy of any Source Code or Executable Code. An electronic signature remains attached to Executable Code so that it will always be possible to know from which Source Code the deployed Executable Code was derived.

61. Once Source Code is available in the Dedicated Transparency Center, the Source Code will be reviewed. The purpose of the review will be to identify any malicious code, bugs, “backdoors,” or exploits that have been written into the Source Code as well as non-malicious vulnerabilities that sometimes result from the normal code development processes.⁴⁶

62. The NSA requires TTUSDS and Oracle to retain yet another U.S.-based security vendor who specializes in reviewing source code to conduct the Source Code security review within the Secure Oracle Cloud. The NSA calls this security vendor the Source Code Inspector.⁴⁷

⁴⁴ See NSA Sec. 9.2.

⁴⁵ See NSA Sec. 9.2.

⁴⁶ See NSA Sec. 9.5.

⁴⁷ See NSA Sec. 9.11.

63. TTUSDS, Oracle, and the Source Code Inspector are charged with ensuring that there is nothing malicious in any Source Code provided by ByteDance.⁴⁸ This review must be conducted on every single piece of Source Code that is required to operate the entirety of what is known as “TikTok”—i.e., the App itself and all software required for the Platform, including the Recommendation Engine.⁴⁹ It also includes any updates, patches, or new versions of the App or the Platform. The review must be completed for any version of the App or Platform that is deployed in the U.S., and the reviewed Source Code must match the SBOM that was delivered with it.⁵⁰

64. Any indication of malicious code or exploit or any deviation from the SBOM must be reported to the U.S. Government.⁵¹ TTUSDS and Oracle will require ByteDance to fix any security problem identified during the Source Code review and will report the outcome to the U.S. Government.⁵² All security fixes or revisions performed by ByteDance must go back through the Source Code review process.⁵³

65. If ByteDance does not correct an identified security problem to the satisfaction of TTUSDS, Oracle and the U.S. Government, the NSA gives Oracle unilateral authority to suspend the use of the App and the Platform in the U.S.⁵⁴

⁴⁸ See NSA Secs. 2.4, 9.5-9.13, 9.15.

⁴⁹ See NSA Sec. 9.7, 9.13.

⁵⁰ See NSA Secs. 9.7, 9.10, 9.12.

⁵¹ See NSA Sec. 9.6.

⁵² See NSA Sec. 9.10.

⁵³ See NSA Secs. 9.7, 9.10, 9.12-9.14.

⁵⁴ See NSA Secs. 9.14-9.15.

66. Once Oracle signs off on reviewed Source Code for the App, Oracle will build Executable Code from the secured and signed Source Code.⁵⁵ This will be done exclusively in the Secure Oracle Cloud.⁵⁶

67. As for the Executable Code for the Platform, it is reviewed by Oracle and built and deployed by TTUSDS. The NSA requires that the Platform be deployed on and operate exclusively in the Secure Oracle Cloud.⁵⁷ The NSA requires TTUSDS and Oracle to ensure that the Platform connects only to Content Delivery Networks⁵⁸ located in the U.S. that have no affiliation with Petitioners when delivering content within the United States.⁵⁹

68. Once Oracle has built secure Executable Code for the App itself, it will use the secure version to deploy the App on the website in the U.S., which will be hosted within the Secure Oracle Cloud, and to the major app stores (e.g., Apple and Google) servicing TikTok U.S. Users.⁶⁰ TTUSDS and Oracle will ensure that only the reviewed versions of the App are made available in the U.S. The version of the App deployed by Oracle will be configured to allow connections only to the Platform in the Secure Oracle Cloud and to no other network or platform. Any movement of content or Public Data from TikTok U.S. Users to or from the rest of the world will be routed through the Platform in the Secure Oracle Cloud before transiting to Content Delivery Networks that carry the traffic globally.⁶¹ Oracle will monitor all

⁵⁵ See NSA Secs. 8.4, 9.10, 9.12.

⁵⁶ See *id.*

⁵⁷ See NSA Secs. 8.4, 8.5, 11.5.

⁵⁸ Content Delivery Networks are servers and related infrastructure that are used for the delivery of static and live content to the TikTok U.S. App. See NSA Sec. 1.5.

⁵⁹ See NSA Secs. 8.4, 8.5.1.i.

⁶⁰ See NSA Secs. 8.4, 9.8, 9.10.

⁶¹ See NSA Secs. 8.4, 8.5, 11.2.

interconnections between the Platform and the rest of the world and can block any such interactions that, in its discretion, are unexpected or unauthorized.⁶² Oracle will also be responsible for assessing and reporting to the U.S. Government on an ongoing basis any risks posed to U.S. national security and User privacy identified in the course of its Source Code review.⁶³

69. The NSA requires that all Protected Data provided or derived from use of the App, including data voluntarily provided by TikTok U.S. Users at registration and any heuristic or behavioral data gathered from use of the App, be transported from the App to the Platform in the Secure Oracle Cloud.⁶⁴ TTUSDS and Oracle will ensure that Protected Data is stored exclusively within the Secure Oracle Cloud and nowhere else, and Oracle will be charged with securing and monitoring all access to the stored Protected Data.⁶⁵ TTUSDS will control all requests for access, including requests pursuant to court orders or subpoenas. The NSA requires that no one outside the U.S. be allowed to view or have access of any Protected Data, including any employee of TTUSDS, Oracle, or a Dedicated Transparency Center located in a “Five Eyes” country, subject to limited exceptions under a set of “Limited Access Protocols.”⁶⁶

70. The NSA requires that TTUSDS make a complete list of all vendors and third parties that provide services, code, or content related to the App or the Platform, and the TTUSDS Security Directors, with oversight from the Third-Party Monitor, must conduct a

⁶² See NSA Secs. 8.5, 9.8, 9.17, 9.18.

⁶³ See NSA Sec. 9.18.

⁶⁴ See NSA Secs. 8.4, 11.5.

⁶⁵ See NSA Secs. 8.4, 9.8, 11.5.

⁶⁶ See NSA Secs. 11.8-11.9.

security review of each vendor, with disclosure of the list to the U.S. Government for review and approval.⁶⁷

71. The NSA requires TTUSDS to establish a Content Advisory Council of external social media, free speech, and content moderation experts who are U.S. citizens.⁶⁸ TTUSDS and the Content Advisory Council will review a so-called “playbook” created by Petitioners that informs how the Recommendation Engine decides what content to recommend to particular users, both global users and TikTok U.S. Users. A copy of the “playbook” will also be given to the U.S. Government and Oracle. TTUSDS will have ultimate say on how the playbook and Recommendation Engine for the TikTok U.S. Platform make decisions for the App and will ensure that the Recommend Engine is trained exclusively within the Secure Oracle Cloud.⁶⁹ Oracle will test the Recommendation Engine to ensure it complies with the playbook, as reviewed and approved by TTUSDS and the Content Advisory Council.⁷⁰

72. In addition to relying on TTUSDS, Oracle, and the Source Code Inspector to carry out NSA functions, the NSA contains heavy oversight monitoring and audit provisions, which will be carried out by yet three more independent U.S.-based entities that must be engaged by TTUSDS. These additional U.S. entities must be approved by and will have reporting and fiduciary responsibilities to the U.S. Government. They cannot have any prior involvement or contractual relationship with Petitioners.

⁶⁷ See NSA Secs. 13.1-13.5.

⁶⁸ See NSA Sec. 5.4.

⁶⁹ See NSA Sec. 9.13.

⁷⁰ See *id.*

73. The first of these is a Third-Party Monitor, which will be responsible for conducting ongoing oversight of the actual implementation of the NSA by TTUSDS, Oracle, and the Source Code Inspector.⁷¹ The Third-Party Monitor will be a principal point of contact for the U.S. Government regarding compliance.⁷² Second, the NSA requires a Third-Party Auditor to conduct an independent audit of compliance by Petitioners and TTUSDS upon request by the U.S. Government.⁷³ The U.S. Government must approve the audit plan. Finally, the NSA requires a Cybersecurity Auditor, which will conduct a more tailored technical audit of TTUSDS's and Oracle's compliance with implementation of the Source Code review processes, the establishment and operations of Dedicated Transparency Centers, the secure Build process, the deployment of the App, the deployment of the Platform in the Secure Oracle Cloud, and the storage and protection of Protected Data.⁷⁴

74. In addition to this oversight, the U.S. Government retains the right to monitor all of Petitioners' and TTUSDS's compliance directly and to conduct inspections at its discretion. The U.S. Government can "inspect the books and records, equipment, servers, and facilities, and premises owned, leased, managed, or operated in the United States by [Petitioners as well as TTUSDS] for the purposes of monitoring compliance with or enforcing this Agreement; provided that in exigent circumstances, no advance notice is required. This right to access and inspect extends to the Personnel, books and records, equipment, servers, facilities, and premises of any third-party contractor or agent working on behalf of [Petitioners and any of their

⁷¹ See NSA Secs. 16.1-16.6.

⁷² See NSA Sec. 16.4.

⁷³ See NSA Sec. 15.1.

⁷⁴ See NSA Secs. 14.1-14.6.

Affiliates].”⁷⁵ The U.S. Government also retains access and inspection rights with respect to Oracle and its compliance with the NSA.⁷⁶

75. The final critical element of the NSA is its collection of enforcement mechanisms. I have already mentioned one of them above—i.e., the ability of Oracle unilaterally to stop use of the App if ByteDance fails to fix security problems with the Source Code.⁷⁷ In addition to this provision related to Source Code review, the NSA contains a provision that authorizes the U.S. Government to shut down operations of the App and the Platform if (i) there are material violations of the NSA, (ii) Petitioners attempt to interfere with any aspect of the NSA, (iii) Oracle is denied access to the Dedicated Transparency Centers, (iv) there is any attempt by Petitioners to deploy any version of the App or Platform that has not been reviewed or deployed by Oracle, or (v) there is any actual or attempted unauthorized access to Protected Data.⁷⁸ In my experience with mitigation agreements, the magnitude of this unilateral enforcement authority given to the U.S. Government is unprecedented.

Caveats and Assumptions

76. I now turn to analyzing the effectiveness of these terms of the NSA, in light of the risk model. However, before doing so, it is important to state certain caveats and assumptions.

77. I note that the only information I have relied upon in preparing this Declaration is the CFIUS record provided by Petitioners to the U.S. Government as well as widely accepted and publicly available facts. My opinion is based solely on those sources and not on anything

⁷⁵ See NSA Sec. 17.1.

⁷⁶ See NSA Sec. 17.2.

⁷⁷ See NSA Secs. 9.14-9.15.

⁷⁸ See NSA Secs. 21.3-21.5.

confidential or unavailable to the public. I have had no access to any classified information regarding this matter. Neither my description of the risk model nor my opinions herein are derived from or rely on classified or non-public information.

78. My first important assumption relates to the “threat” element of the risk model. I will assume for purposes of this Declaration that Petitioners are subject to at least influence if not control by Chinese interests. I understand that Petitioners disagree with this assumption, but analysis of this question is not within the scope of this Declaration. Based on this assumption, I will also assume without analyzing or opining that Congress and CFIUS considered Petitioners to pose HIGH threats.

79. In light of this assumption about Petitioners, I also assume without analyzing or opining that Congress and CFIUS would not be willing to trust Petitioners to faithfully comply with the NSA in the absence of some means of either ensuring trust or removing the requirement to trust Petitioners, such as the use of a trusted third party to be responsible for mitigation implementation.

80. My final assumption relates to the “consequences” posed by Petitioners control of or access to the App or the Platform. I will assume for purposes of this Declaration that if Protected Data is compromised or if the App or Platform is used to exploit content on the Platform, the national security consequences will be HIGH. Again, I am not analyzing this question and offer no opinion on the magnitude of the asserted consequences one way or the other. I understand Petitioners may disagree with this assessment, but the resolution of this question is not necessary to my analysis.

Analysis of the NSA

81. Because I am assuming a HIGH threat posed by Petitioners and a HIGH consequence to national security if vulnerabilities are exploited, my analysis is focused exclusively on the vulnerability analysis under the risk model. The seminal question is whether the NSA, if faithfully implemented as written, is sufficient to effectively mitigate vulnerabilities associated with Petitioners' control of the App and Platform, including access to Protected Data, such that the overall vulnerability assessment would be reduced to a LOW level.

82. As discussed above in connection with the risk model, the vulnerability analysis asks whether, by virtue of controlling a U.S. company or asset, a foreign "threat" actor would have sufficient access to allow it to capitalize and implement methods of exploitation to impair national security. In this case, the question is whether Petitioners could use their control, influence, or access to exploit the App or Platform to (i) use Protected Data to gather intelligence about U.S. persons, or (ii) use the Platform, including control of the Recommendation Engine, to engage in propaganda or misinformation campaigns either in China's favor or against the U.S.

83. As a threshold matter, I first consider whether the U.S. Government would be required to rely on Petitioners to faithfully comply with the NSA in order to mitigate national security risks. To reiterate, the U.S. Government has been reluctant to enter into mitigation agreements with companies based in China or under Chinese control because of concern that the Chinese government could force companies to subvert U.S. national security interests despite the existence of contractual mitigation requirements. The important exception to this reluctance has been where the U.S. Government has been able to rely on a trusted third party to ensure compliance such that blind reliance on a Chinese company is not required.

84. That is the case here. First, the NSA requires the creation of TTUSDS, which will have governance and operational independence. Its Board and management will be free from the control or influence of Petitioners. TTUSDS will be responsible for the core security functions (i.e., “CFIUS Functions”) that are at the heart of the NSA’s mitigation mechanisms.

85. Second, importantly, the NSA requires the use of a third-party TTP—Oracle—to be the technical overseer of the NSA and to deploy and operate the App and the Platform. Oracle is a trusted U.S. company, and under the terms of the NSA, Oracle will have responsibilities directly to the U.S. Government. Its economic incentives will align with U.S. Government interests because non-compliance could lead to the U.S. Government exerting its shut-down authority under the NSA, which would end what is certainly well-compensated work by Oracle under the master services agreement.

86. By using TTUSDS and Oracle, the U.S. Government is not required to rely on Petitioners’ compliance. It effectively means that U.S. citizens with obligations and loyalties to the U.S. Government will be in control of NSA implementation.

87. It is relevant to re-emphasize that this use of a secure U.S. subsidiary of a foreign parent is a well-recognized and long-used method for addressing national security risks. CFIUS has often used it, as has the FCC and “Team Telecom.” It is also used often by the Department of Defense to protect classified information and classified contracts from the control and influence of foreign parent companies.

88. The next step in the analysis is to look at whether Petitioners could still have sufficient access to exploit the App or the Platform, despite not having control or influence over TTUSDS or any of the mechanisms for deploying or operating the App or the Platform.

89. In the absence of Board or management control, a relevant question is whether Petitioners might still have the ability to manipulate or control the placement of co-opted employees in TTUSDS or Oracle or to influence decisions regarding vendors associated with the App or the Platform. The NSA effectively cuts off these vectors by imposing rules around TTUSDS hiring and controlling the ability of TTUSDS to use employees who are non-U.S. citizens or who have had a prior affiliation with Petitioners. These same hiring and vendor rules are imposed on Oracle.

90. Because the NSA cuts off these governance, management, and hiring/contracting vectors, the lone remaining potential access that could enable exploitation by Petitioners is through technical exploits of the App or the Platform. For purposes of clarity, it is important to re-emphasize that under the NSA, ByteDance will remain completely in control of developing Source Code for all of the components that comprise “TikTok”—the App and the Platform, including the Recommendation Engine. As stated above, I am assuming without concluding that this access could be used for exploiting vulnerabilities, such as misappropriating Protected Data or manipulating content on the TikTok Platform.

91. With that said, in my professional opinion, the NSA effectively cuts off this technical “access” vector and effectively mitigates the ability of Petitioners to exploit the App or the Platform. There are two technical access methods to consider. The first is whether by virtue of understanding the Source Code for the App and the Platform, Petitioners or some other third-party could gain control over and access to deployed Executable Code and configuration of the App and the Platform. The second is whether there may be self-executing functions, “backdoors,” or other exploits planted in the Source Code that could exploit the App or the

Platform even if Petitioners could not take control following deployment or control configuration.

92. On the first point—Petitioners using deployed Executable versions of the App and the Platform—as explained above, the NSA requires that all deployment and operations of the App and the Platform must emanate from and be controlled by TTUSDS within the Secure Oracle Cloud, including all application and network configurations. Oracle’s infrastructure will be the exclusive source in the U.S. for issuance of the App and the Platform. Petitioners will have no physical or logical access to the App or the Platform once signed Source Code and accompanying SBOMs are deposited in Dedicated Transparency Centers. All functionality and all interconnectedness for the Platform will be hosted on and run through the Secure Oracle Cloud. There may not be a more secure commercial cloud environment in the U.S. than the Secure Oracle Cloud. The NSA’s terms ensure that there will be no logical or physical access or interconnection points between the App and the Platform and any untrusted entity because TTUSDS, with Oracle serving as a trusted validator, will control the end-to-end process. Oracle will be able to view, inspect, and stop any traffic between the App and the Platform and well as all movement of Protected Data. Under the direction of TTUSDS, Oracle will have technical operational responsibility for the storage, protection, and control of Protected Data.

93. The second consideration relates to embedded self-executing exploits in the Source Code. As discussed at length above, a key component of the NSA is the Source Code review process. This falls under the responsibility of TTUSDS, Oracle, and an additional Source Code Inspector. It will be conducted within the Secure Oracle Cloud, after pulling Source Code and SBOMs from the Dedicated Transparency Centers. Oracle will enable the Source Code

Inspector to have full manual and automated access. No Source Code will enter the Build process until it is reviewed by Oracle.

94. Source Code review is a difficult and detailed process. However, highly trained reviewers are adept at understanding code. Automated tools for helping review code have greatly enhanced the effectiveness of Source Code review, including new tools empowered by artificial intelligence.

95. While it is hypothetically possible that some security flaws or even exploits could slip through the Source Code review process, it would be implausible as a practical matter for Petitioners to attempt to evade the NSA by embedding malicious code. First, there is a high likelihood of discovery. Both Oracle and the Source Code Inspector will be very highly trained in spotting malicious code, especially when using robust tools. The reviewers are experienced in spotting both intentionally malicious code as well as non-malicious vulnerabilities that emerge during the coding process.

96. Second, there will be immediate reporting to the Third-Party Monitor and the U.S. Government if malicious code is found.

97. Third, the use of SBOMs and signed code means that Oracle and the Source Code Inspector will be able to track the provenance of malicious code and identify quickly where it came from and when it arrived. Oracle and the Source Code Inspector will also be able to compare versions of Source Code that it reviewed and will be able to see when new features or commands have been added or removed, all of which will have to comport with SBOMs that accompany the reviewed Source Code.

98. All of this will enable not only reporting under the terms of the NSA, but if there is malicious intent or an attempt to compromise a protected computer or network, it could

become a federal criminal matter under the federal computer intrusion statute and, depending on the facts, could also be investigated or prosecuted as an attempt by a foreign power to take action against U.S. interests under national security statutes.

99. In addition, the NSA imposes rigorous broad oversight over the NSA's implementation, mandating the involvement of three additional independent monitors and auditors—the Third-Party Monitor, the Third-Party Auditor, and the Cybersecurity Auditor.

100. The provisions in the NSA that give the U.S. Government the ability to unilaterally stop the use of the App and the Platform for non-compliance is a high-water mark for U.S. Government control in a mitigation environment. The fact that there are six independent U.S. entities involved in NSA implementation and compliance—TTUSDS, Oracle, the Source Code Inspector, the Third-Party Monitor, the Third-Party Auditor, and the Cybersecurity Auditor—means that if any one of those entities catch or alert on non-compliance, it could trigger the process that could result in the U.S. Government putting a stop to the App and the Platform. It is a very broad net and would be a significant and complex set of obstacles to navigate even if there were an intent by Petitioners—or some other Chinese interest—to surreptitiously exploit vulnerabilities via the Source Code or the deployed App or Platform.

101. In addition to my experience and expertise with CFIUS and mitigation agreements, I am also a former counterespionage investigator and prosecutor. In my experience related to nation-state intelligence gathering efforts, when a potential avenue for intelligence collection is highly scrutinized and spotlighted, there are strong incentives to choose an alternate method and avoid detection. The App and the Platform are under intense scrutiny. The NSA will accelerate the scrutiny and visibility in an exponential manner. I believe Chinese interests,

even if they were otherwise motivated to want to exploit the App and the Platform, would choose alternate vectors of collection in order to avoid discovery.

102. My final point of analysis relates to the Recommendation Engine and the potential manipulation of content on the Platform to disseminate propaganda, squelch information that is harmful to Chinese interests, or foment disunity within the U.S. Access vectors for Petitioners to exploit this vulnerability, if they were to retain control of the Platform, would be to embed functionality in the Source Code for the Recommendation Engine or to manipulate the configuration of the Recommendation Engine, including feeding “training” data into it in an effort to sway how content is distributed. The NSA contains several provisions that would make misuse of the Recommendation Engine unlikely. First, the Source Code review likely will find security flaws. More importantly, the Recommendation Engine will be accompanied by a playbook that will be available to TTUSDS and Oracle, as well as to the Content Advisory Council, on how recommendations to users should look. The Third-Party Monitor will also be involved and will enable the U.S. Government to have a say in the playbook. Oracle, which will have complete and exclusive control of the deployed Recommendation Engine in the U.S., will be required to monitor its behavior against the playbook. Oracle will conduct testing and analysis to assess its behavior. In addition, all of the training (i.e., machine learning) for the Recommendation Engine will be done in the Secure Oracle Cloud using only training data in that Cloud, which means there will be no opportunity to train the Recommendation Engine on Chinese propaganda or misinformation. Only U.S. persons will be involved in the deployment and training of the Recommendation Engine.

103. Similar protections exist with respect to other processes for the promotion or filtering of TikTok content apart from the Recommendation Engine. The NSA requires

TTUSDS to ensure that only authorized personnel can engage in video promotion and filtering for the App and Platform and to document for the Third-Party Monitor how video promotion and filtering functions will be carried out. The Third-Party Monitor and the Third-Party Auditor can conduct audits to ensure promotion and filtering decisions are consistent with the playbook and other policies and are properly geared toward commercial purposes. Reports of those audits will be provided to the U.S. Government, which can conduct its own audits.

104. To be clear, I do not assess any one provision of the NSA as the single “silver bullet” that renders the NSA effective to mitigate national security risk. Rather, it is the combination of the level of independence granted to TTUSDS, reliance on multiple trusted third parties such as Oracle, the operational security processes, complex and thorough technical mitigations, as well as unprecedented oversight, monitoring, and very rigorous enforcement mechanisms, that lead me to conclude that the NSA effectively mitigates national security risk associated with the App and the Platform. Using the risk model described above, if the NSA were implemented as written, the overall vulnerability assessment associated with Petitioners owning and deploying the TikTok U.S. App and the TikTok U.S. Platform would be reduced to a LOW level. I cannot conceive of a more technically secure mitigation scheme for the App and the Platform in the U.S. than the scheme devised by the NSA.

CONCLUSIONS

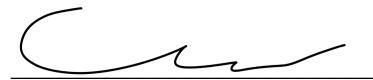
105. The risk model described above is the national security analytic model that is used by Congress, CFIUS, and other U.S. government entities to assess the effectiveness of the NSA to mitigate national security risk.

106. I have reviewed the NSA as well as the history of negotiations between CFIUS and Petitioners regarding the NSA.

107. Using the risk model, my professional opinion is that if implemented as written, the NSA would effectively mitigate the U.S. national security risks associated with Petitioners owning and deploying the TikTok U.S. App and the TikTok U.S. Platform.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this day June 17, 2024.


Christopher P. Simkins

Appendix 1

Chris Simkins is an entrepreneur, lawyer, and advisor with decades of experience working at the intersection of business and the U.S. Government's national security interests. He has deep legal, operational, and technical experience with regulatory processes that protect technology and information. He has counseled hundreds of companies ranging from the Fortune 500 to start-ups on CFIUS, DCSA, and other security matters and has designed and implemented security mitigation programs to protect against nation-state attacks.

Mr. Simkins is also an experienced entrepreneur, having founded and served as CEO for multiple companies. He is currently the CEO and founder of Laconia Law & Consulting, which provides legal, consulting, advisory, and operational services to companies. He was the co-founder and CEO of Corsha, a cybersecurity company that secures machine-to-machine communications, and Chain Security, a professional services company that identifies vulnerabilities in technology supply chains and designs and implements technical and operational mitigation programs. He is currently the CEO and co-founder of Shouldrs, Inc., a tech start-up building an AI-powered platform that autonomously performs back-office functions for small businesses.

Positions Held:

- 2023-Present Co-Founder & CEO, Shouldrs, Inc.
- 2008-Present Founder & CEO, Laconia Law & Consulting
- 2023-Present Director & Chair of Government Security Committee, Zetec, Inc.
- 2024-Present Leadership Council, National Small Business Association
- 2017-2023 Co-Founder & CEO and Strategic Advisor, Corsha, Inc.
- 2011-2017 Co-Founder & CEO, Chain Security, LLC
- 2007-2008 Senior Counsel, Covington & Burling
- 2006-2007 Senior Counsel to the Assistant Attorney General, Criminal Division and National Security Division, U.S. Department of Justice
- 2004-2006 Counterespionage Section, U.S. Department of Justice
- 1998-2004 Counsel (and Associate), WilmerHale

Education:

- 1997 Brigham Young University Law School, J.D.
magna cum laude, Order of the Coif, Managing Editor of BYU Law Review
- 1994 Brigham Young University, B.A., Political Science
magna cum laude

Patents:

- Co-Inventor, Pat. No. US10992651B2 ("Streaming authentication using chained identifiers")
- Co-Inventor, Pat. No. US11343243B2 ("Machine-to-machine streaming authentication of network elements")
- Co-Inventor, Pat. No. US20230006841A1 ("Machine-to-machine cryptographic material rotation")

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC.

and

BYTEDANCE LTD.,

Petitioners,

v.

No. 24-1113

MERRICK B. GARLAND, in his official
capacity as Attorney General of the
United States,

Respondent.

DECLARATION OF STEVEN WEBER

I, Steven Weber, under penalty of perjury, hereby declare as follows:

1. I am a Professor of the Graduate School at the University of California, Berkeley (“UC Berkeley”), where I hold joint appointments as Professor at the School of Information and in the Department of Political Science. I am also the founder and former faculty director of the Center for Long Term Cybersecurity at UC Berkeley, where for seven years I led a multi-disciplinary research group that worked on emerging digital security issues at the confluence of new technologies, human behavior, and risk calculations made by firms and governments. In addition to my academic appointments, I am a Partner at Breakwater Strategy, a strategic insights and communications firm, where I assist clients with strategic decision-making and communications in areas that involve the intersection of technology and public policy. I received a Ph.D. in political science from Stanford University in 1989 and have been a professor at UC Berkeley since 1989.

2. My work focuses on U.S. national security issues with particular emphasis on how digital technologies impact and are impacted by national and international security. I have written three relevant university press peer-reviewed books and a number of peer-reviewed journal articles on this subject, as well as many other articles published in non-peer reviewed publications. I have served as a consultant to a wide variety of U.S. and global firms as well as U.S. government agencies dealing with strategic issues at the intersection of national security and the digital economy. A copy of my curriculum vitae is attached hereto as Appendix 1.

3. I have been retained by counsel for Petitioners TikTok Inc. and ByteDance Ltd. in this action to analyze certain reported justifications for the Protecting Americans from Foreign Adversary Controlled Applications Act (the “Act”), which was signed into law by President Biden on April 24, 2024. As I discuss below in greater detail, I understand that some have

suggested justifications for the Act focused on two issues: (1) the security of the data that TikTok collects from its U.S. users, particularly as it relates to alleged risks of disclosure to the Chinese government; and (2) the possibility that TikTok's recommendation algorithm (*i.e.*, the computer code that selects what content to present in a user's feed) could be misused for the benefit of the Chinese government, either by censoring certain content or promoting propaganda or disinformation.¹

4. As I discuss below, these issues are not unique or even distinctive to TikTok. (By TikTok, I mean to refer to the platform as opposed to any particular corporate entity.) It is inherent in digital technologies that every company, governmental entity, or non-governmental organization faces risks to the security of the data that it creates, processes, transmits, and stores—whether on behalf of employees, customers, or others.² Major companies (including many with highly sophisticated security operations) such as Yahoo!, LinkedIn, Meta, Marriott, Experian, Adobe, UnitedHealth, and many others have suffered well-known data breaches of millions of user records.³ And with respect to TikTok's recommendation algorithm, I am unaware of any evidence that supports the contention that TikTok's algorithm has been manipulated to promote propaganda or disinformation. Insofar as there is a concern that propaganda or disinformation *exists* on the platform, that is an issue that essentially all social

¹ Because the Act does not contain any legislative findings or a statement of purpose, I have reviewed statements from individual Members of Congress as well as other sources expressing possible justifications for the Act.

² See, e.g., *Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts*, U.S. Dep't of Homeland Security (May 15, 2018), <https://perma.cc/EDJ4-Y3DP>.

³ Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO Online (Nov. 8, 2022), <https://perma.cc/T3U4-8TPU>; see also Manas Mishra & Zeba Siddiqui, *UnitedHealth Says Hackers Possibly Stole Large Number of Americans' Data*, Reuters (Apr. 22, 2024), <https://perma.cc/2DPZ-ZJUK>.

media and entertainment platforms are dealing with more generally—a fact the U.S. government has acknowledged in official intelligence reports.⁴ YouTube, for example, has previously added disclaimers to certain channels that were reportedly being used to spread disinformation on behalf of the Russian government.⁵ Meta issues quarterly reports on its efforts to respond to coordinated inauthentic behavior on its platforms and, in a recent report, announced that it had removed thousands of accounts originating in China and Russia that had engaged in coordinated inauthentic behavior in 2023.⁶ Indeed, it is now common practice among major social media firms to work to identify and take down content and accounts that promote disinformation and to make regular public disclosures in which they offer details on these operations.⁷

5. In short, while there are legitimate policy issues regarding data security and the use of online platforms for propaganda and disinformation, they are industry-wide issues that are not unique to TikTok. Indeed, even if TikTok were able to implement the type of “qualified divestiture” contemplated by the Act, the concerns that animated the Act would remain, just as they do with respect to many other social media and entertainment platforms. To the extent that TikTok is different from its peers, moreover, it is distinguished by the commitments it has made to address the U.S. government’s stated concerns, which are expressed in the draft National

⁴ Nat’l Intel. Council, Declassified Intelligence Community Assessment, *Foreign Threats to the 2020 U.S. Federal Elections* (Mar. 10, 2021), <https://perma.cc/JKF3-7KDC>.

⁵ Paresh Dave & Christopher Bing, *Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels: Researchers*, Reuters (June 7, 2019), <https://perma.cc/SB9H-R76W>.

⁶ Ben Nimmo, Nathaniel Gleicher, Margarita Franklin, Lindsay Hundley & Mike Torrey, *Third Quarter Adversarial Threat Report*, Meta (Nov. 2023), <https://perma.cc/R9HW-Y49Y>.

⁷ See, e.g., *YouTube Community Guidelines Enforcement*, Google (last accessed June 12, 2024), <https://perma.cc/33PU-QN6S>; *Transparency Reports*, Meta (last accessed June 17, 2024), <https://perma.cc/AJE9-YWPL>; *Transparency Report*, July 1, 2023–December 31, 2023, Snap (last accessed June 12, 2024), <https://perma.cc/Q629-WU9K>; *Covert Influence Operations*, TikTok (last accessed June 12, 2024), <https://perma.cc/EF89-NNDH>.

Security Agreement and reflect protections for the integrity of TikTok data and content that go beyond industry norms.

6. With this introduction, I address in detail the two issues that have been cited by some Members of Congress as justifications for the Act: data security and the susceptibility of TikTok’s algorithm to foreign government influence.

I. Data Security

7. The first justification that some have suggested for the Act is a perceived need to protect U.S. TikTok users’ “data security.”⁸ According to a House Committee Report for an earlier version of the Act, mobile applications, including those purportedly controlled by foreign adversaries, can “collect vast amounts of data on Americans.”⁹ The House Committee Report expressed a concern that data collected through mobile applications could be used by a foreign adversary to “conduct espionage campaigns,” including by tracking specific individuals.¹⁰

8. As an initial matter, the assertion that mobile applications, including TikTok, “collect vast amounts of data on Americans” is principally a statement about data privacy, not data security. There is a separate policy debate about the extent to which social media and other digital product companies collect information from users, and this debate is beyond the scope of my testimony. I note, however, that the type and amount of data that TikTok collects from U.S. users—which is disclosed to users pursuant to TikTok’s Privacy Policy, to which users agree as a

⁸ Jane Coaston, *What the TikTok Bill Is Really About, According to a Leading Republican*, N.Y. Times (Apr. 1, 2024), <https://perma.cc/B2YN-7QFK> (quoting the Act’s original sponsor, Representative Mike Gallagher).

⁹ H.R. Comm. on Energy & Com., *Protecting Americans from Foreign Adversary Controlled Applications Act*, H.R. Rep. No. 118-417 at 2 (2024) (hereinafter, the “House Committee Report”).

¹⁰ *Id.* at 2, 4.

condition of signing up for the app—is comparable to the type and amount of data that other social media platforms and applications collect from U.S. users.¹¹ In other words, the data collected by TikTok is not meaningfully different—either in amount or kind—from the data that other applications collect, including applications owned by U.S. companies like Google, Snap, and Meta.¹²

9. Social media and online entertainment platforms are also not unique in collecting data from users. A wide variety of mobile applications collect significant amounts of user data, such as weather apps that collect precise geolocation data and device information.¹³ Indeed, some apps have been shown to collect categories of information that bear little or no relationship to the business purpose of the app at all—such as utility apps (like a flashlight app on a cell phone) that collect geolocation and other non-pertinent data.¹⁴

¹¹ Milton L. Mueller & Karim Farhat, *TikTok and U.S. National Security*, Georgia Inst. of Tech. Internet Governance Project, at 19 (2023), <https://perma.cc/JR3Z-F5TK> (explaining that “TikTok’s behavior is not suspicious and it is not exfiltrating unusual data” and that “[w]hile TikTok collect[s] many data items, overall they still fall within general industry norms for user data collection” (citation omitted)).

¹² It is worth noting that, in some respects, TikTok collects more limited data than other mobile applications. For example, the current version of the TikTok app does not collect precise or approximate GPS data from U.S. users. *See Mythbusting: The Facts on Reports about Our Data Collection Practices*, TikTok (Feb. 22, 2023), <https://perma.cc/GS8A-W9FC>. Additional transparency around the data TikTok collects is now also available by virtue of TikTok storing such data in the Oracle Corporation cloud environment, as discussed below.

¹³ Thorin Klosowski, *We Checked 250 iPhone Apps—This Is How They’re Tracking You*, N.Y. Times (May 6, 2021), <https://perma.cc/9YS5-AECB>; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), <https://perma.cc/B5AU-YLKP>.

¹⁴ *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, Fed. Trade Comm’n (Dec. 5, 2023), <https://perma.cc/KN96-7TTL>.

10. Although the assertion that TikTok “collect[s] vast amounts of data on Americans” is primarily a statement about data privacy, the assertion that user data collected by TikTok could be used by a foreign adversary to “conduct espionage campaigns” is an assertion about data security because it is a statement regarding who has access to data and for what purpose. The validity of this statement can therefore be analyzed based on principles of data security.

11. Before proceeding with the analysis, there are two general information security principles that should be kept in mind. First, data security is not a binary switch that can be toggled on or off. There are always tradeoffs being made among three components of security: confidentiality, integrity, and availability of data.¹⁵ As with many enterprise risks, data security is an exercise in risk management—identifying risks, assessing them, and mitigating those risks to acceptable levels.¹⁶

12. Second, when it comes to data security threats, it is virtually impossible to prove the negative and establish that there are *no* risks associated with a particular application, network, or data storage and management system.¹⁷ Sophisticated organizations and information security professionals base their work on the foundational proposition that malicious actors and technology are constantly evolving, which means the threat landscape is always changing. Even

¹⁵ This three-part framework is explained by the National Institute of Standards and Technology in *Standards for Security Categorization of Federal Information and Information Systems*, Fed. Info. Processing Standards Publication 199 (Feb. 2004), <https://perma.cc/52R4-XE3H>.

¹⁶ *Cybersecurity Strategy*, U.S. Dep’t of Homeland Security (May 15, 2018), <https://perma.cc/5UUV-ZVE7>; Nat’l Inst. of Standards & Tech., *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 Rev. 5, at 13 (Sept. 2020), <https://perma.cc/KY6M-4TF9>.

¹⁷ Shuman Ghosemajumder, *You Can’t Secure 100% of Your Data 100% of the Time*, Harv. Bus. Rev. (Dec. 4, 2017), <https://perma.cc/22XX-DQLU>.

an organization with state-of-the-art security practices across the board cannot, with full confidence, assert that there is no risk that its data could be vulnerable to attack or inadvertently accessed, improperly accessed, or disclosed. These principles form the basis of sophisticated data security programs and strategies in advanced organizations.

13. With these general principles in mind, turning to the specific asserted national security concerns related to TikTok's user data, it is important to first assess the type of data we are discussing. As a recent report by the Internet Governance Project at the Georgia Institute of Technology ("Georgia Tech") explained, "[f]ull access to all TikTok data would provide [an actor with] aggregate data about the user population's video uploading and consumption behavior."¹⁸ As the report explained, while such information may be "commercially valuable" to TikTok as well as certain developers and advertisers, it is unlikely to be particularly valuable to a foreign state like China, as it provides no "special insight into the control of critical infrastructure, military secrets, opportunities for corporate espionage, or knowledge of weapons systems."¹⁹

14. Even assuming some national security-related intelligence value for high-value targets (*e.g.*, individuals of particular interest from an intelligence perspective) could be derived from collecting a data set of commercially-focused information, the notion that the Chinese government would seek to amass this intelligence information by appropriating TikTok user data is not plausible, given the alternative means available to a nation state interested in acquiring information about individuals in another country. Those alternatives include conducting open source intelligence gathering from public information sources (including LinkedIn, Facebook,

¹⁸ Mueller & Farhat, *supra* n.11, at 20.

¹⁹ *Id.*

and other platforms) where people regularly disclose information about themselves that could be valuable to an intelligence program; and direct cyberattack operations like China's reported intrusion into the database of the U.S. Office of Personnel Management ("OPM") as well as Russia's reported theft of certain email correspondence between U.S. government agencies and Microsoft through a breach of Microsoft's software systems.²⁰

15. Another avenue by which a nation-state actor may acquire information about high-value targets is by purchasing such information on the open market. Historically, there has been little regulation of the U.S. data brokerage industry, which is comprised of thousands of companies that collect, sell, and distribute individuals' data. At the same time as it passed the Act, Congress also passed legislation that places certain restrictions on data brokers' ability to transfer certain categories of information to "foreign adversary countr[ies]" (defined to include China, Russia, Iran, and North Korea) as well as entities "controlled" by such foreign adversary countries.²¹ The legislation, however, does not forestall a foreign adversary's ability to purchase U.S. user data through the broader, multilayered data brokerage market. The recently passed legislation, for example, applies only to "data broker[s]," a statutorily defined term with enumerated exceptions.²² Commentators have also noted that the legislation does not regulate

²⁰ Josh Fruhlinger, Ax Sharma & John Breeden, *15 Top Open-Source Intelligence Tools*, CSO Online (Aug. 15, 2023), <https://perma.cc/7TTFG-KSCH>; Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO Online (Feb. 12, 2020), <https://perma.cc/L9SV-N6SY>; Sean Lyngaas, *Russian Hackers Steal U.S. Government Emails with Microsoft, Officials Confirm*, CNN (Apr. 11, 2024), <https://perma.cc/P7DF-96EV>.

²¹ H.R. 815, div. I, § 2(a), 118th Cong., Pub. L. No. 118-50 (Apr. 24, 2024).

²² *Id.* § 3. For example, the legislation defines a "data broker" to include entities that "sell[], license[], rent[], trade[], transfer[], release[], disclose[], provide[] access to, or otherwise make[] available data of United States individuals, that the entity did not collect directly from such individuals." *Id.* Entities that sell the "data of United States individuals" that they themselves "collect directly from such individuals" fall outside the definition.

the sale of U.S. user data to intermediary entities who may, in turn, sell or provide the purchased data to foreign adversaries.²³ Given these and other limitations, there are still a variety of ways by which a nation-state actor, like China, can obtain U.S. user data from the data broker ecosystem, notwithstanding the recent enactment of legislation designed to regulate brokers.

16. Given the existence of more effective and efficient means of obtaining relevant information about high-value targets, it is unlikely that China would seek to compel TikTok to turn over user data for intelligence-gathering purposes. Data security professionals generally work from the proposition that attackers will choose the path of least resistance to achieve their objectives. A review of cybersecurity breaches over the last decade bears this assumption out: the vast majority of attacks are not the most technically sophisticated operations (that often receive the most attention among specialists), but are instead much simpler attacks carried out through mundane vulnerabilities, such as unchanged default passwords and the lack of two-factor authentication.

17. Another reported reason for the Act is TikTok's asserted ties to China, which Members of Congress have suggested increase the vulnerability of U.S. TikTok data to misappropriation. A House Committee Report for an earlier version of the Act asserts that because affiliates of TikTok Inc.'s parent company, ByteDance Ltd., are headquartered in China and employ Chinese citizens, TikTok user data is less secure than data collected and maintained by other apps and platforms.²⁴ According to the report, under Chinese law, "the [Chinese

²³ Justin Sherman, *The Pros and Cons of the House's Data Broker Bill*, Lawfare (Apr. 11, 2024), <https://perma.cc/5BTM-FW9N>.

²⁴ House Committee Report at 3–4. TikTok has pointed out that ByteDance Ltd. is a Cayman Islands holding company, and that its operating entities in China are subsidiaries of ByteDance Ltd. References in this declaration to "ByteDance" are to the corporate group, rather than any particular entity.

government] can require a company headquartered in [China] to surrender all its data to the [Chinese government], making companies headquartered [in China] an espionage tool of the CCP [Chinese Communist Party].”²⁵ The report further contends that TikTok “rel[ies] on . . . engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application,” “potentially expos[ing] U.S. users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development.”²⁶ Finally, the report contends that ByteDance “has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.”²⁷

18. From a data security perspective, these asserted ties to China do not distinguish TikTok from other multinational corporations that create, maintain, and utilize U.S. user data. With respect to the concern that the Chinese government may require ByteDance to surrender data on U.S. TikTok users, it bears emphasis that many U.S. technology companies—including Cisco, Dell, Electronic Arts, Hewlett-Packard, IBM, LiveRamp, and Palo Alto Networks—have Chinese-headquartered subsidiaries, and therefore face the same theoretical risk that Chinese government officials may seek to compel disclosure of customer or user data from those companies.²⁸ Moreover, a number of apps and platforms that appear to have connections to and

²⁵ *Id.* at 4; see also *Threat Posed by TikTok*, U.S. Dep’t of Justice (Mar. 6, 2024) (“[The Chinese government’s] national security law requires any company doing business in China to make its data accessible to the [Chinese] government and to support its intelligence efforts.”).

²⁶ House Committee Report at 5.

²⁷ *Id.* at 7.

²⁸ Cisco Systems, Inc., Annual Report (Form 10-K) (Sept. 7, 2023); Dell Technologies Inc., Annual Report (Form 10-K) (Mar. 25, 2024); Electronic Arts Inc., Annual Report (Form 10-K) (May 22, 2024); HP Inc., Annual Report (Form 10-K) (Dec. 15, 2023); International Business Machines Corporation, Annual Report (Form 10-K) (Feb. 26, 2024); LiveRamp Holdings, Inc.,

operations in China—such as Temu and Shein, two popular e-commerce apps in the United States—collect and maintain U.S. user data as well.²⁹

19. With respect to the concern that ByteDance relies on “engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application,” many U.S. companies maintain software and other engineering operations in China. Electronic Arts, for example, maintains a major development studio in China that, as of June 2024, has over 400 employees.³⁰ These employees, many of whom are Chinese citizens, work on developing popular video games, such as FIFA and The Sims,³¹ both of which have millions of U.S. and international users.³² Such companies’ Chinese operations reflect that the issues identified in the House Committee Report are, once again, not unique to TikTok, but instead are industry-wide issues. Indeed, companies face risks that “engineers and back-end support” may engage in “problematic activities tied to source code development,” regardless of whether those companies have offices or operations in China. For example, earlier this year, a former Google software engineer based in California was indicted on charges of stealing trade secrets related to

Annual Report (Form 10-K) (May 22, 2024); Palo Alto Networks, Inc., Annual Report (Form 10-K) (Sept. 1, 2023).

²⁹ Nicholas Kaufman, *Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes*, U.S.-China Econ. & Security Review Comm’n (Apr. 14, 2023), <https://perma.cc/8X32-DSDR>; Mark A. Green, *It Isn’t Just TikTok: Americans Like Other Chinese-Owned Apps Too*, Wilson Ctr. (May 2, 2023), <https://perma.cc/Z5FT-MV7G>.

³⁰ *EA China*, Electronic Arts (last accessed Jun. 12, 2024), <https://perma.cc/Y43K-GKKV>.

³¹ *Id.*

³² *The Sims 4 Becomes the Most Widely Played Game in the 23 Year History of the Franchise With More Than 70 Million Players Worldwide*, Electronic Arts (Apr. 18, 2023), <https://perma.cc/57E4-K2JD>; *FIFA 23*, Active Player (last accessed Jun. 12, 2024), <https://perma.cc/8937-UEZ5>.

artificial intelligence systems in development at Alphabet, allegedly to benefit two Chinese companies the engineer was secretly working for.³³

20. Finally, the fact that ByteDance reportedly employs certain CCP members is likewise not a distinguishing feature of TikTok. As U.S. government officials have acknowledged, virtually all major Chinese companies are required to maintain internal committees comprised of CCP members, and in recent years, a number of U.S. companies doing business in China have instituted such committees of their own.³⁴ There is evidence that many of these CCP committees are purely symbolic in nature.³⁵ But even if they are not, the assertion that ByteDance maintains an internal CCP committee does not distinguish the company from other companies with CCP committees (including both Chinese and U.S. companies) that are not treated the same way as TikTok under the Act.

21. There is one material respect, however, in which it is possible to distinguish TikTok from other industry participants when it comes to the data security concerns that were

³³ Karen Freifeld & Jonathan Stempel, *Former Google Engineer Indicted for Stealing AI Secrets to Aid Chinese Companies*, Reuters (Mar. 6, 2024), <https://perma.cc/F4PZ-JHW3>.

³⁴ Christopher Wray, *The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States*, Hudson Inst. (July 7, 2020), <https://perma.cc/4JNC-N3AY>; John K. Costello, Mem. for the Secretary, Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942 (Sept. 17, 2020), at 7 (noting that, as of 2017, CCP committees “existed in around 70 percent of 1.86 million private owned companies in China”).

³⁵ Joris Mueller, Jaya Wen & Cheryl Wu, *The Party and the Firm*, Working Paper (Dec. 2023), at 2, 5–6, <https://perma.cc/P3YV-V88S> (explaining that “[p]arty influence is more rhetorical than behavioral among domestic private and foreign-owned firms”); Lauren Yu-Hsin Lin & Curtis Milhaupt, *Party Building or Noisy Signaling? The Contours of Political Conformity in Chinese Corporate Governance*, 50 J. Legal Stud. 187, 189–90 (2021) (explaining that privately owned enterprises in China that have adopted charters providing for internal CCP committees “have largely limited their adoptions to symbolic provisions” and have not “acced[ed] to institutionalized party involvement in corporate governance”).

raised by Members of Congress, and that is the company's efforts to address the U.S. government's concerns through a national security agreement. I have reviewed the draft National Security Agreement ("NSA") that TikTok Inc. negotiated with the Committee on Foreign Investment in the United States ("CFIUS"), which I understand was designed to alleviate certain national security concerns identified by CFIUS concerning the U.S. TikTok platform. I am not an expert on the CFIUS process in particular, and I am not offering an opinion on the CFIUS review in this case. In my view, however, the relevance of the draft NSA is not limited to the specific confines of the CFIUS process. Rather, the draft NSA can be assessed more broadly as a set of commitments intended to mitigate a set of perceived national security risks, and the effectiveness of the draft NSA can also be analyzed on those terms, without regard to the specific parameters of the CFIUS review process.

22. Analyzing the draft NSA on those terms, it is my opinion that it provides for a robust system of controls to mitigate data security risks that might arise were foreign governments or adversarial groups acting as their agents to attempt to access protected U.S. user data. Moreover, in my view, these proposals significantly exceed and improve upon the controls that have been proposed and reportedly implemented by other social media and technology companies, including U.S. companies.

23. Pursuant to the NSA, TikTok Inc. has agreed to form a special-purpose subsidiary, TikTok U.S. Data Security Inc. ("USDS"), to oversee security-related issues.³⁶ USDS would be overseen by a special board of Security Directors, whose appointment would be subject to the U.S. government's approval.³⁷ The NSA further provides that protected U.S. user

³⁶ NSA arts. 2, 3, 8 & 11.

³⁷ *Id.* § 3.1.

data would be stored in the cloud environment of a U.S.-government-approved partner, Oracle Corporation (“Oracle”), with access to such data managed exclusively by USDS.³⁸ The NSA also provides for an extensive, independent third-party cybersecurity audit with multiple layers of review.³⁹ The NSA also includes a “shut-down option” that would allow the U.S. government to suspend TikTok in the United States if TikTok Inc. does not abide by certain obligations under the agreement.⁴⁰

24. I understand that TikTok Inc. has started voluntarily implementing certain provisions of the NSA, including by incorporating and staffing USDS and partnering with Oracle on the migration of the U.S. TikTok platform and protected U.S. user data to the Oracle cloud environment.⁴¹ I am not aware of any other online platform or service that maintains organizational and functional data security controls of the kind that have been proposed under the NSA.⁴²

³⁸ *Id.* arts. 8 & 9.

³⁹ *Id.* § 14.1.

⁴⁰ *Id.* §§ 21.3–5.

⁴¹ *About Project Texas*, TikTok (last accessed June 12, 2024), <https://perma.cc/W8Q5-F5Y6>.

⁴² Zoom Video Communications (“Zoom”), for example, has adopted some—but not all—of the protocols contemplated by the draft NSA. Zoom has created a separate product—Zoom for Government—that includes security features beyond those included in Zoom’s standard product and processes communications “exclusively in continental U.S. data centers that are managed solely by U.S.-based, U.S. people.” Josh Rogin, *The White House Use of Zoom for Meetings Raises China-Related Security Concerns*, Wash. Post (Mar. 3, 2021), <https://perma.cc/M5GV-NS6Z>. TikTok, by contrast, is restructuring the company to maintain a version of the TikTok platform for the United States in a U.S. subsidiary; erecting software barriers to isolate the U.S. version of the TikTok app within the Oracle cloud; and granting Oracle—a U.S. company—access to its underlying source code.

25. Members of Congress have expressed particular concerns about the ability of the Chinese government to use TikTok to track specific individuals, including journalists.⁴³ This concern appears to be based on press reports that a few ByteDance employees used their previous access to certain TikTok user data to attempt to determine whether certain U.S.-based journalists were meeting with TikTok personnel who were suspected of leaking confidential information.⁴⁴ As with the other data security issues discussed above, the data security concerns raised by this episode relate to an industry-wide issue: the potential access to, and misuse of, data by corporate insiders for purposes not authorized by company policy. For example, Google has reportedly terminated dozens of employees between 2018 and 2020 for abusing their access to the company's tools or data, including with respect to accessing Google user data.⁴⁵ As another example, in November 2022, Meta reportedly fired or disciplined more than two dozen employees and contractors who inappropriately took control of Facebook user accounts.⁴⁶ And Uber has settled claims related to the company's "God View" tool, which reportedly allowed employees to track the location of Uber riders without obtaining their permission.⁴⁷ Indeed, even

⁴³ House Committee Report at 4, 8.

⁴⁴ Emily Baker-White, *Lawmakers Express Outrage that TikTok Spied on Journalists*, Forbes (Dec. 23, 2022), <https://perma.cc/G8ZF-ERR6>; Emily Baker-White, *TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022), <https://perma.cc/45YP-QVPK>; Mitchell Clark & Alex Heath, *TikTok's Parent Company Accessed the Data of US Journalists*, The Verge (Dec. 22, 2022), <https://perma.cc/N4EJ-DHXX>.

⁴⁵ Joseph Cox, *Leaked Document Says Google Fired Dozens of Employees for Data Misuse*, Vice (Aug. 4, 2021), <https://perma.cc/96LZ-39DH>.

⁴⁶ Rohan Goswami, *Meta Reportedly Disciplined or Fired More than Two Dozen Workers for Taking Over Facebook User Accounts*, CNBC (Nov. 17, 2022), <https://perma.cc/GY4Q-6D72>.

⁴⁷ Chris Welch, *Uber Will Pay \$20,000 Fine in Settlement Over 'God View' Tracking*, The Verge (Jan. 6, 2016), <https://perma.cc/43QZ-42UK>; Brian Fung, *Uber Settles with FTC Over 'God View' and Some Other Privacy Issues*, L.A. Times (Aug. 15, 2017), <https://perma.cc/U82U-4B44>.

outside the technology industry, the potential misuse of customer data by corporate insiders is a compliance challenge for virtually all companies.⁴⁸

26. In the case of TikTok, it has been reported that the company investigated the misconduct, disclosed its findings, took action against the employees involved, and implemented remediation efforts, including a restructuring of the department in which the employees involved in the misconduct were employed and reforms meant to strengthen the company's internal controls.⁴⁹ This is consistent with how other companies have handled incidents of this kind.⁵⁰ From a data security perspective, TikTok's actions reflect an industry-best-practice response to an economy-wide compliance challenge, not a unique and extraordinary national security threat that would support consideration of an outright ban or divestment of the platform involved.⁵¹

II. Susceptibility of TikTok's Algorithmic Recommendation System to Outside Influence

27. The second justification that some have suggested for the Act pertains to TikTok's algorithmic recommendation system, which certain Members of Congress have

⁴⁸ *Credit Suisse Staffer Took Salary Data*, Reuters (Feb. 13, 2023), <https://perma.cc/DHR2-7NYQ> (reporting that former Credit Suisse staffer misappropriated employee salary data as well as bank account information, Social Security numbers, and addresses); *Supermarket Morrisons Sued by Staff Over Personal Data Leak*, BBC News (Oct. 9, 2017), <https://perma.cc/CJQ9-M6CG> (reporting that former grocery store employee misappropriated employees' personal data).

⁴⁹ David Shepardson, *ByteDance Finds Employees Obtained TikTok User Data of Two Journalists*, Reuters (Dec. 22, 2022), <https://perma.cc/499P-JWHE>.

⁵⁰ Cox, *supra* n.45; Goswami, *supra* n.46.

⁵¹ The arbitrariness of the Act's approach to data security is underscored by the Act's exemption for companies that operate a website or application "whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews." See Act § 2(g)(2)(B). Websites or applications that "allow users to post product reviews, business reviews, or travel information and reviews" also frequently collect data from users. I am unaware of any national security-based reason for exempting companies that maintain such websites and applications from coverage under the Act.

suggested could be used to disseminate propaganda or otherwise mislead the American public.⁵² For example, Representative Mike Gallagher, one of the Act’s co-sponsors, stated that TikTok presents a “propaganda threat” to the United States by “placing the control of . . . information—like what information America’s youth gets—in the hands of America’s foremost adversary [*i.e.*, China].”⁵³ Representative Raja Krishnamoorthi, another of the Act’s co-sponsors, stated that “the [TikTok] platform continue[s] to show dramatic differences in content relative to other social media platforms.”⁵⁴ And Representative Chip Roy, a member of the House Select Committee on the CCP, stated that “[TikTok] is . . . poisoning the minds of our youth every day on a massive scale.”⁵⁵ These statements could be construed to suggest that foreign actors, including China, may be using TikTok to influence users’ allegiances or belief systems by promoting and/or censoring certain content; alternatively, they could be interpreted as criticisms of the content available on TikTok irrespective of any such alleged manipulation. For purposes of this declaration, I focus on the allegation that TikTok is being used to manipulate users’ belief systems in furtherance of the aims of a foreign actor.

28. Before assessing these specific allegations, it is important to be clear about the applicable terminology. Specifically, it is important to draw a threshold distinction between “censorship” and “content moderation.” The two concepts are not the same. The issue around

⁵² House Committee Report at 2, 7–8.

⁵³ Coaston, *supra* n.8 (quoting Representative Gallagher).

⁵⁴ Sapna Maheshwari, David McCabe & Annie Karni, *House Passes Bill to Force TikTok Sale from Chinese Owner or Ban the App*, N.Y. Times (Mar. 13, 2024), <https://perma.cc/3C6F-7P4V>.

⁵⁵ Press Release, U.S. House Select Comm. on Strategic Competition between the U.S. and the Chinese Communist Party, Gallagher, Bipartisan Coalition Introduce Legislation to Protect Americans from Foreign Adversary Controlled Applications, Including TikTok (Mar. 5, 2024), <https://perma.cc/Q7DH-853D>.

censorship here is whether an algorithm is being used to downgrade, remove, or prevent the creation of content that expresses opinions that the censor finds objectionable for illegitimate reasons. Content moderation, by contrast, refers to the legitimate removal or restriction of content that violates platforms' stated policies and the law. Here again, the practice of content moderation is an industry-wide issue and not an issue or practice limited to TikTok. X (formerly known as Twitter) attempts to block violence-promoting tweets.⁵⁶ Meta has an evolving set of policies that attempt to block various kinds of hate speech.⁵⁷ YouTube has modified its content moderation policies in an attempt to reduce radicalization, and in fact, the company reports that it removed over 9 million videos from the site in the 3-month period spanning October to December 2023.⁵⁸

29. It is similarly important to draw a distinction between “propaganda” and “content recommendation” or “content promotion.” Much like the discussion of censorship, the issue of propaganda here is whether an algorithm is being used to promote or distribute content in order to influence or manipulate an audience for some illegitimate purpose. Content recommendation or promotion, by contrast, refers to the recommendation and/or promotion of certain content to users for legitimate business purposes. Here again, the practice of content recommendation and promotion is an industry-wide phenomenon. For example, for many years, YouTube partnered with creators to create original content for the site, which the company distributed through its

⁵⁶ *The X Rules*, X (last accessed June 12, 2024), <https://perma.cc/RJL9-62CS>.

⁵⁷ *Community Standards*, Facebook (last accessed June 12, 2024), <https://perma.cc/5CMJ-UWCK>.

⁵⁸ *YouTube Community Guidelines Enforcement* (last accessed June 12, 2024), YouTube, <https://perma.cc/8P6N-W6Q5>.

YouTube Originals page.⁵⁹ Instagram uses a variety of artificial intelligence tools to select, rank, and deliver content to a user's "Explore" page, which has a clear business purpose, to facilitate users' access to content they might like.⁶⁰

30. From a national security perspective, the question is whether the algorithm is legitimately shaping the flow of content in accordance with a commercial product strategy, along with appropriate restrictions to counter proscribed activity (such as hate speech) consistent with its public Terms of Service; or whether the algorithm is illegitimately seeking to manipulate perspectives and opinions in directions that serve a foreign state's short- and long-term strategic interests, which may be at odds with those of the United States.

31. Specifically with regard to TikTok, the question can be stated as follows: Is there evidence and reason to believe that TikTok is now or would become essentially an algorithmic propaganda tool of the Chinese government or the Chinese Communist Party? Based on the information that I have reviewed, my answer to this question is "no."

32. As an initial matter, a small number of anecdotes about allegedly "censored" or "promoted" content do not in and of themselves demonstrate either the use of a platform for propaganda purposes or, even more so, a national security risk. That is partly because algorithmic content moderation and user experience customization are based on a fast-evolving science that involves state-of-the-art machine learning techniques to solve some of the hardest problems in content recognition, natural language processing, and other technology that sometimes go under the label of "artificial intelligence." Like humans, algorithms can make

⁵⁹ Todd Spangler, *YouTube Shuts Down Original Content Group*, Variety (Jan. 18, 2022), <https://perma.cc/B7AD-CADB>.

⁶⁰ *How Posts Are Chosen for Explore on Instagram*, Instagram (last accessed June 12, 2024), <https://perma.cc/M9LG-YVEE>.

mistakes and then learn from those mistakes. In most companies, algorithmic moderation is supplemented by human content moderators who typically make assessments about “gray” or uncertain cases where algorithmic decision-making is ambiguous or inconsistent, as well as overseeing how algorithms perform relative to the platforms’ policies. The question, accordingly, is whether and how social media platforms react and evolve as they develop their technologies and practices over time and in response to ambiguous cases, concerns, complaints, and errors.

33. TikTok Inc.’s commitments in the draft NSA indicate that it is willing to respond to concerns about content moderation. For example, the NSA provides that all content moderation on the TikTok U.S. platform—both human and algorithmic—would be subject to third-party verification and monitoring.⁶¹ Moreover, the NSA provides that the TikTok U.S. platform and application would be deployed through the Oracle cloud infrastructure, and Oracle and another third-party partner (to be approved by the U.S. government) would have access to TikTok’s source code.⁶² Oracle and the third-party partner would review and vet TikTok’s source code and conduct inspections and tests of TikTok’s recommendation algorithm to ensure that it is acting in conformance with TikTok’s publicly stated, published content policies.⁶³ Oracle would report the findings of its inspections to the Security Directors (discussed above), after which the NSA contemplates that TikTok and Oracle would work to implement any necessary changes to TikTok’s software based on Oracle’s findings.⁶⁴

⁶¹ NSA §§ 5.4, 9.13, 16.6.

⁶² *Id.* §§ 8.4, 9.1, 9.11.

⁶³ *Id.* § 9.13.

⁶⁴ *Id.*

34. Once again, I am unaware of any other major social media or entertainment platform that has committed to the level of transparency and extensive controls proposed under the NSA.

35. Recent academic studies further indicate that TikTok is honoring its commitment to responsible and viewpoint-neutral content moderation practices, notwithstanding certain anecdotal press reports to the contrary. For example, a 2023 report from Georgia Tech’s Internet Governance Project (referenced above) found that videos depicting “content . . . known to be major Communist Party taboos,” including “[s]upport for Hong Kong democracy protesters,” were “easily . . . found on TikTok,”⁶⁵ rebutting earlier press reports that such videos were uncommon on TikTok.⁶⁶ The report also found that searches related to the Chinese government’s treatment of the Uyghur minority, an ethnic minority group based in China’s Xinjiang Province, produced a list of search terms and videos “that by themselves are likely illegal on Chinese social media.”⁶⁷ Such evidence indicates that TikTok is neither promoting pro-China content nor censoring content that may be critical of China in a systematic way that supports allegations of a propaganda or disinformation campaign.

36. Certain Members of Congress—including Senator Mitt Romney and Representative Mike Lawler—have suggested that passage of the Act was motivated, at least in part, by concerns that TikTok has promoted pro-Palestinian content in the aftermath of Hamas’s

⁶⁵ Mueller & Farhat, *supra* n.11, at 12–13.

⁶⁶ Drew Harwell & Tony Romm, *Inside TikTok: A Culture Clash Where U.S. Views about Censorship Often Were Overridden by the Chinese Bosses*, Wash. Post (Nov. 5. 2019), <https://perma.cc/HX57-WYRK>.

⁶⁷ Mueller & Farhat, *supra* n.11, at 13.

October 7, 2023 attacks on Israel and the ongoing conflict in Gaza.⁶⁸ This assertion, however, rests on faulty inferences drawn from data—including the number of videos on TikTok with purportedly pro-Palestinian hashtags as compared to videos with pro-Israeli hashtags—that has been taken out of context. For example, it has been reported that, as of late October 2023, videos posted with the hashtag “standwithpalestine” had 10 times as many views on TikTok as videos posted with the hashtag “standwithisrael.”⁶⁹ But subsequent reporting has clarified that this 10-to-1 statistic includes view counts from TikTok users located outside of the United States as well as view counts dating back to 2020, well before the October 7 attacks.⁷⁰ This is significant because reporting has shown that videos with pro-Palestinian hashtags are overwhelmingly created and viewed by users outside of the United States,⁷¹ and pro-Palestinian hashtags are older and more established than pro-Israeli hashtags.⁷² In other words, the 10-to-1 statistic is not an accurate characterization of the videos posted and viewed on TikTok in the United States—and

⁶⁸ Ben Metzner, *Mitt Romney Reveals the Twisted Reason Why Congress Moved to Ban TikTok*, The New Republic (May 6, 2024), <https://perma.cc/VV6Y-QEYV> (quoting Senator Romney); Will Bunch, *Is TikTok Ban to Stop Kids Learning about Gaza?*, Phila. Inquirer (May 7, 2024), <https://perma.cc/3D2N-ERYL> (quoting Representative Lawler).

⁶⁹ David Ingram & Kat Tenbarger, *Critics Renew Calls for a TikTok Ban, Claiming Platform Has an Anti-Israel Bias* (Nov. 1, 2023), NBC News, <https://perma.cc/U2MW-BJSR>.

⁷⁰ *Id.*

⁷¹ Louise Matsakis & J.D. Capelouto, *Asian & Middle Eastern Users Tilt TikTok Balance Toward Palestinians*, Semafor (Nov. 3, 2023), <https://perma.cc/U5BL-XVEF>.

⁷² *The Truth about TikTok Hashtags and Content During the Israel-Hamas War*, TikTok (Nov. 13, 2023), <https://perma.cc/KE8G-98S2>; see also Paul Matzko, *Lies, Damned Lies, and Statistics: A Misleading Study Compares TikTok and Instagram*, Cato Inst. (Jan. 2, 2024), <https://perma.cc/KK77-HN2X> (criticizing study comparing the use of political hashtags on TikTok and Instagram insofar as the study failed to control for how long each platform existed and thus the time period over which certain political hashtags were used on each platform).

most importantly does not accurately describe data about what U.S. users were seeing—after the October 7 attacks.⁷³

37. A review of U.S. hashtag data for the month after the October 7 attacks shows that only a slightly higher number of videos with pro-Palestinian hashtags were posted to the U.S. TikTok platform as compared to videos with pro-Israeli hashtags.⁷⁴ Moreover, the view counts for these sets of videos were roughly the same.⁷⁵ Indeed, an analysis by TikTok shows that videos with pro-Israeli hashtags received 68% more views per video in the United States than videos with pro-Palestinian hashtags.⁷⁶ And third-party analyses based on TikTok’s Research API—a data set comprised of public data that TikTok makes available to researchers—similarly show that videos with pro-Israeli hashtags and/or hashtags associated with content about the Israeli-Palestinian conflict that is neither pro-Israeli nor pro-Palestinian generally received more views per video in the weeks and months after the October 7 attacks as compared to videos with pro-Palestinian hashtags.⁷⁷ This suggests that, in general, videos posted with pro-Israeli hashtags received as many or more views per video on TikTok than videos with pro-Palestinian hashtags.⁷⁸ These statistics undercut the claim that TikTok is somehow “promoting” pro-Palestinian content on the app.

⁷³ It should also be noted that analyses based on hashtag data have certain limitations. For example, hashtags are assigned by users and do not always accurately reflect the subject matter of the videos to which they are assigned. Users may also post videos without hashtags.

⁷⁴ Ingram & Tenbarger, *supra* n.69.

⁷⁵ *Id.*; see also EJ Dickson, *Is TikTok Really Boosting Pro-Palestinian Content?*, Rolling Stone (Nov. 12, 2023), <https://perma.cc/K6NV-RXJ2>.

⁷⁶ *The Truth about TikTok Hashtags*, *supra* n.72.

⁷⁷ Laura Edelson, *Getting to Know the TikTok Research API*, Cybersecurity for Democracy (last accessed June 12, 2024), <https://perma.cc/V3AJ-8JEP>.

⁷⁸ Ingram & Tenbarger, *supra* n.69; Dickson, *supra* n.75.

38. Even if there were significantly more pro-Palestinian content on TikTok, the presence of such content does not demonstrate or in any manner prove that TikTok's recommendation algorithm is "promoting" a pro-Palestinian message. Rather, the prevalence of such content may simply be a function of the demographics of TikTok's user base, which trends younger than other platforms.⁷⁹ This is significant because recent polling shows that young people are less likely to support Israel's actions following the October 7 attacks as compared to older individuals, with one poll finding that only 20% of 18-to-24-year-olds support Israel's reaction to the attacks, as compared to 58% of respondents aged 50 years or older.⁸⁰ More broadly, the polling trends show that young people's support for Israel has been decreasing over the last 10 years—a trend that pre-dates TikTok's existence and even more so its widespread popularity.⁸¹ In other words, the evidence does not support the conclusion that TikTok is the cause of young people's lower levels of support for Israel, as opposed to a reflection of pre-existing trends.⁸²

⁷⁹ Monica Anderson Michelle Faverio & Jeffrey Gottfried, *Teens, Social Media & Technology 2023*, Pew Research Center (Dec. 11, 2023), <https://perma.cc/3PKM-NXAT> (finding that a greater percentage of teenagers use TikTok than any other social media application or entertainment platform, with the exception of YouTube); Rebecca Jennings, *TikTok Isn't Creating False Support for Palestine. It's Just Reflecting What's Already There.*, Vox (Dec. 13, 2023), <https://perma.cc/B5KE-KMQ8> (reporting that approximately 60% of TikTok's U.S. monthly active users are between 16 and 24 years old and another 26% are between 25 and 44 years old).

⁸⁰ *Sympathy Grows for Palestinians but Majority Still Sympathize More with Israelis, Quinnipiac University National Poll Finds; Generational Divide Widens on View of Israel*, Quinnipiac Univ. Poll (Nov. 16, 2023), <https://perma.cc/B7QS-FC67>.

⁸¹ Lydia Saad, *Young Adults' Views on Middle East Changing Most*, Gallup (Mar. 24, 2023), <https://perma.cc/83J2-YD6U>.

⁸² To the extent Members of Congress have cited the incidence of pro-Palestinian content on TikTok as compared to other platforms, *see, e.g.*, Metzner *supra* n.68, it is important to note that comparing the type and volume of content across different applications can be difficult, including because different platforms have different user numbers, serve different markets and

39. Certain Members of Congress have also cited the existence of videos on TikTok reciting, discussing, or reacting to Osama bin Laden’s “Letter to America” as a reason for voting in favor of the Act.⁸³ Content related to bin Laden’s letter, however, is not unique to TikTok. Other social media platforms saw increased engagement with bin Laden’s letter in the aftermath of the October 7 attacks, indicating that the letter presented an industry-wide issue.⁸⁴ The temporary virality of the letter may also be a function of a media “feedback loop” that is a familiar phenomenon of social media. According to public reports, engagement with TikTok videos regarding bin Laden’s letter increased dramatically only after media reports about the existence of such content on the app, suggesting that interest in the videos stemmed in substantial measure from media reports on other platforms about the existence of the videos as opposed to the popularity of such content on its own, let alone efforts by TikTok to promote or disseminate

demographics, and were founded at different times, *see* Matzko, *supra* n.72. Moreover, different platforms make different types of data publicly available. Even so, there are public reports that there is significantly more content with pro-Palestinian hashtags on Facebook and Instagram as compared to content with pro-Israeli hashtags. *See, e.g.,* Drew Harwell, *TikTok Was Slammed for Its Pro-Palestinian Hashtags. But It’s Not Alone*, Wash. Post. (Nov. 13, 2023), <https://perma.cc/6CYQ-GE3N> (reporting that, as of November 2023, there were 39 times as many posts on Facebook with the #freepalestine hashtag as compared to posts with the #standwithisrael hashtag; on Instagram, there were 26 times as many posts with the #freepalestine hashtag as compared to posts with the #standwithisrael hashtag).

⁸³ *See, e.g.,* Maheshwari *et al.*, *supra* n.54 (quoting Representative Krishnamoorthi). In his “Letter to America,” written in 2002, bin Laden purports to explain why al Qaeda attacked the United States on September 11, 2001. In doing so, bin Laden criticizes the U.S. government’s involvement in the Middle East and its support for Israel. *See* Bobby Allyn, *The Story Behind the Osama bin Laden Videos on TikTok*, NPR (Nov. 17, 2023), <https://perma.cc/U9FS-BY5E>.

⁸⁴ *See* Daysia Tolentino, *TikTok Removes Hashtag for Osama bin Laden’s “Letter to America” after Viral Videos Circulate*, NBC News (Nov. 16, 2023), <https://perma.cc/4BHJ-48YL> (reporting a 4,300% increase in references to bin Laden on X between November 14 and 16, 2023, and a 400% increase in searches for bin Laden on YouTube over the same period).

such content.⁸⁵ The reported temporary virality of the letter may also have resulted from efforts by malicious actors to manipulate platforms' recommendation engines. Such conduct is a well-documented phenomenon that exists across many different platforms and is not limited to TikTok.⁸⁶

40. Other Members of Congress have cited TikTok's March 2024 decision to display a pop-up message urging users to contact their representatives about the Act as a reason for voting in favor of the Act's provisions.⁸⁷ According to Representative Krishnamoorthi, TikTok's action "transformed a lot of lean yeses into hell yeses."⁸⁸ Here again, however, TikTok's actions do not distinguish TikTok from other companies and, in fact, reflect industry-wide practices. In response to a proposal by then-New York City Mayor Bill de Blasio to restrict the number of Uber drivers allowed to operate in New York City, Uber added an option on its app that allowed users to select a "DE BLASIO" ride, which Uber suggested would resemble the app experience if Mayor de Blasio's measure passed.⁸⁹ Among other things, the "DE BLASIO" option informed users that their ride would arrive in 25 minutes.⁹⁰ In 2012, Google displayed a blacked-out logo on its homepage along with a message directing users to "Tell Congress: Please don't censor the

⁸⁵ Drew Harwell & Victoria Bisset, *How Osama bin Laden's "Letter to America" Reached Millions Online*, Wash. Post (Nov. 16, 2023), <https://perma.cc/29VS-QBML>.

⁸⁶ Christian Kastner, *Security and Privacy in ML-Enabled Systems*, Medium (Dec. 20, 2022), <https://perma.cc/9BNW-2JAF>.

⁸⁷ Sapna Maheshwari, David McCabe & Cecilia Kang, *"Thunder Run": Behind Lawmakers' Secretive Push to Pass the TikTok Bill*, N.Y. Times (Apr. 24, 2024), <https://perma.cc/BR72-P779> (quoting Representative Krishnamoorthi).

⁸⁸ *Id.*

⁸⁹ Christopher Spata, *Uber Slams NYC Mayor with New "DE BLASIO" Feature*, Complex (Jul. 16, 2015), <https://perma.cc/T3ZQ-SRUS>.

⁹⁰ *Id.*

Web.”⁹¹ Google’s temporary change to its homepage responded to certain legislation pending in Congress at the time, which Google believed would “impose huge regulatory costs and stifle innovation on the Web.”⁹² Such actions are not materially different from TikTok’s asserted efforts to mobilize its user base in response to the Act’s introduction. In each instance, it was left to users whether to engage in the democratic activity of contacting their representatives.

41. Finally, it bears mention that the Act’s treatment of TikTok stands in contrast to its treatment of foreign-owned news applications, including applications owned by Xinhua News (China), RT News (Russia), and NewsBreak (China), that operate in the United States.⁹³ RT News has been publicly identified by the U.S. Department of State as “play[ing] an important role within Russia’s disinformation ecosystem” and, according to the Department of State, serves as a “conduit[] for Kremlin talking points aimed at influencing foreign public opinion in a way that benefits Russia’s foreign policy and national security interests.”⁹⁴ Xinhua News, in turn, has been described as the “world’s biggest propaganda agency,”⁹⁵ with the U.S. State Department characterizing Xinhua as a “PRC [People’s Republic of China] propaganda outlet[.]”⁹⁶ And

⁹¹ Michael Cavanaugh, *Google Blacks Out: “Censored” Logo Goes Dark to Oppose SOPA/PIPA Legislation*, Wash. Post (Jan. 18, 2012), <https://perma.cc/V69T-NJGZ>.

⁹² *Id.*

⁹³ See Xinhua News (last accessed June 12, 2024), <https://perma.cc/W4X3-X9GV>; RT News (last accessed June 12, 2024), <https://perma.cc/F4FX-2KE9>; James Pearson, *NewsBreak: Most Downloaded U.S. News App Has Chinese Roots and ‘Writes Fiction’ Using A.I.*, Reuters (June 5, 2024), <https://perma.cc/EE28-NC8C>.

⁹⁴ *Kremlin-Funded Media: RT and Sputnik’s Role in Russia’s Disinformation and Propaganda Ecosystem*, U.S. Dep’t of State Global Engagement Ctr. (Jan. 2022), <https://perma.cc/S9ES-G5GL>.

⁹⁵ *Xinhua: The World’s Biggest Propaganda Agency*, Reporters Without Borders (Oct. 2005), <https://perma.cc/UGB9-M4ES>.

⁹⁶ *Designation of Additional Chinese Media Entities as Foreign Missions*, U.S. Dep’t of State (June 22, 2020), <https://perma.cc/VJS6-5JE6>.

recent reports state that NewsBreak—a subsidiary of a “Chinese news aggregation app” with a China-based engineering team—has become a popular news app in the United States, notwithstanding claims that the app routinely publishes fictitious news stories on its platform.⁹⁷ From a national security perspective, there is no reason to apply one set of rules to applications owned by or affiliated with ByteDance (including TikTok) and another set of rules to applications owned by or affiliated with RT News, Xinhua News, NewsBreak, and similar companies.

III. Conclusion

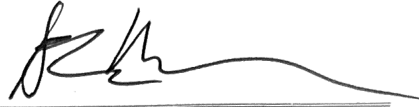
42. Social media and entertainment platforms, like TikTok, raise important policy issues, including the appropriate protection of user data, content moderation, and propaganda. These are legitimate issues to consider from a policy perspective, but they are issues that the industry confronts as a whole and are not unique or distinctive to TikTok.

43. As I have discussed above, TikTok’s approach for dealing with these issues is in line with—and in many respects markedly better than—industry best practices, even for companies that hold significant sensitive user data. In light of the foregoing, there is no evident national security rationale for the Act’s particular focus on TikTok. It is arbitrary to select one market participant for policy issues that an entire industry faces. This is particularly the case where there exist alternative mechanisms—including the mitigation proposals that TikTok Inc. has outlined in the NSA negotiated with CFIUS—that enable the federal government to use regulatory frameworks and establish extensive processes that mitigate data and national security risks around data and algorithms beyond what they would currently be able to achieve with peer firms.

⁹⁷ Pearson, *supra* n.93.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 17th day of June, 2024.

A handwritten signature in black ink, appearing to read 'Steven Weber', is written over a horizontal line.

Steven Weber

APPENDIX 1

STEVEN WEBER

steve_weber@berkeley.edu
+1 415-203-8432

Professor of the Graduate School
UC Berkeley School of Information
203 B South Hall
UC Berkeley, Berkeley CA 94720

Partner
Breakwater Strategy
1299 Pennsylvania Ave Floor 12
Washington DC 20004

Major Fields of Work

International Political Economy
Technology and Data Governance
International Institutions
American Foreign Policy, particularly National Security and FDI Issues
Applications of Cognitive and Behavioral Psychology to Decision-making
Scenarios and Strategic Planning

Education

July 1988 June 1989 Postdoctoral Fellow Center for International Affairs, Harvard University
March 1985 June 1988 Ph.D., Stanford Dept. of Political Science
Sept. 1982 June 87 M.D. Student, Stanford Medical School
Sept 1984 March 85 M.A. Stanford Dept. of Political Science
Sept 1979 June 82 B.A. Washington University (History, International Development)

Administrative Appointments UC Berkeley

Director, Institute of International Studies, 2004-2009
Founder and Director, Center for Long Term Cybersecurity, UC Berkeley, 2015 - 2022
Associate Dean and Head of School of Information, Division of Computing Data Science and Society 2020-2021

Books

Bloc By Bloc: How to Organize a Global Enterprise for the New Regional Order Harvard University Press, 2019.

The End of Arrogance: America in the Global Competition of Ideas Harvard University Press, 2010 (with Bruce Jentleson)

The Success of Open Source Harvard University Press, 2004.

Cooperation and Discord in US-Soviet Arms Control, Princeton University Press, 1991.

Edited Books

Deviant Globalization: Black Market Economy in the 21st Century Continuum Press, 2011 (with Nils Gilman and Jesse Goldhammer)

Globalization and The European Political Economy Columbia University Press, 2001.

European Integration and American Federalism: A Comparative Perspective (with Richard Herr). Berkeley: University of California, International and Area Studies, 1996.

Monographs

Shaping the Postwar Balance of Power 1947/1961: Multilateralism in NATO, UC Berkeley Institute of International Studies, Research Papers in International Affairs, Spring 1991. A shorter version of this monograph appears as a chapter in Multilateralism Matters: The Anatomy of an Institution, edited by John Ruggie, Columbia University Press, 1993.

Cybersecurity Futures 2020. Report issued by the Center for Long Term Cybersecurity UC Berkeley 2015

Coauthored Books

Tracking A Transformation (with BRIE co-authors). Brookings Institution Press, 2001.

The Highest Stakes: Economic Foundations of the New Security Order, Oxford University Press, 1992. (with John Zysman, Micheal Borrus, et. al.

Selected Papers

"Realism, Detente, and Nuclear Weapons", International Organization 44. Winter 1990.

"Cooperation and Interdependence", Daedalus, 120, Winter 1991. [Reprinted in Emmanuel Adler, ed., The Theory and Practice of Arms Control, Johns Hopkins University Press, 1992.]

Origins of the European Bank for Reconstruction and Development. Working Paper Series, Harvard University Center for European Studies, 1992.

"Shaping the Postwar Balance of Power", International Organization 46. Summer 1992.

"Mercantilism and Global Security" (with John Zysman and Michael Borrus), The National Interest, Autumn 1992.

"Origins of the European Bank for Reconstruction and Development", International Organization 48. Winter 1994.

"International Political Economy 'After' The Business Cycle". Journal of Social, Political, and Economic Studies. 21. Fall 1996.

"The Changing Politics of EMU", Swiss Political Science Review. 2. Fall 1996.

"The End of the Business Cycle?" Foreign Affairs July-August 1997.

"Prediction and the Middle East Peace Process", Security Studies 6. Summer 1997.

"Emerging Markets: Good for US? Good for Everyone?" (with Elliot Posner), Brown Journal of International Affairs. Summer 1998.

"Five Scenarios of the Israeli-Palestinian Relationship in 2002," Security Studies 7. Summer 1998 (with Janice Stein et.al.)

"Organizing International Politics: Sovereignty and Open Systems," (with Christopher Ansell) International Political Science Review. January 1999.

"A Certain Idea of Nuclear Weapons: France's Non-Proliferation Policies in Theoretical Perspective," (with Nicolas Jabko), Security Studies 8. Winter 1999.

"God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World," European Journal of International Relations 6. Winter 2000. (with Janice Stein, Ned Lebow, and Steven Bernstein)

"International Organizations and the Pursuit of Justice in the World Economy," Ethics and International Affairs, Winter, 2000.

"Creating a Pan-European Equity Market: The Origins of EASDAQ," Review of International Political Economy Winter 2001 (with Elliot Posner)

"The Political Economy of Open Source Software" BRIE Working Paper # 140, University of California, Berkeley. At <http://brie.berkeley.edu/~briewww/pubs/wp/wp140.pdf> (A shorter version is published in Tracking a Transformation, Brookings Institution, 2001).

"E-Finance and the Politics of Transitions," in "Electronic Finance: A New Perspective and Challenges," BIS Paper No. 7 (Bank of International Settlements, November 2001). (with John Zysman)

"The New Economy and Economic Growth in Developing Countries: Speculations on the Meaning of Information Technology for Emerging Markets", (with John Zysman). Emergo: A Journal of Transforming Economies and Societies, 2003.

"Will Information Technology Reshape the North-South Asymmetry of Power in the Global Political Economy?" (with Jennifer Bussell). Studies in Comparative International Development 40. Summer, 2005.

"Getting to No," (with James Goldgeier), The National Interest, Winter 2006.

"The International Implications of China's Fledgling Regulatory State: From Product Maker to Rule Maker" (with Abraham Newman and David Bach), New Political Economy December 2006.

"How Globalization Went Bad" (with Naazneen Barma, Ely Ratner, and Matthew Kroenig), Foreign Policy 2007.

"A World Without the West," (with Naazneen Barma and Ely Ratner), The National Interest. 2007.

"America's Hard Sell," (with Bruce Jentleson), Foreign Policy 2008.

"A World Without the West: Empirical Patterns and Theoretical Implications," Chinese Journal of International Politics 2, 2009. (with Naazneen Barma, Giacomo Chiozza, and Ely Ratner)

"Taking Soft Power Seriously," Comparative Strategy 2010 (with Matthew Kroenig and Melissa McAdam)

"The Mythical Liberal Order", The National Interest 2013 (with Naazneen Barma and Ely Ratner)

'Visualizing ambivalence: showing what mixed feelings look like'. (with Galen Panger and Bryan Rea) 2013. In CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13). ACM

'Back in the USSR: Is the European Union Heading for a Soviet-Style Collapse?' The American Interest (with Nils Gilman) December 2016

"The New World of Data: Four Provocations on the Internet of Things" (with Richmond Wong), First Monday February 2017.

"Can You Secure an Iron Cage?" (with Nils Gilman and Jesse Goldhammer), Limn 8 2017.

'Coercion in Cybersecurity: What Public Health Models Reveal', Journal of Cybersecurity May 2017

'Data, Development, and Growth,' Business and Politics September 2017

"Moving Slowly, Not Breaking Enough: Trump's Cybersecurity Accomplishments" (with Betsy Cooper), Bulletin of the Atomic Scientists October 2017.

'The Long Game of Chinese Techno-nationalism', (with Shazeda Ahmed), First Monday April 2018.

"Reducing the Waste from our Digital Lives," *Noema*, April 2021 (with Ann Cleaveland et. al.)

"The 2020s Political Economy of Machine Translation," *Business and Politics*, 2022.

'A To-Do List for Web 3 Visionaries' *Noema*, March 2022 (with Arik Ben-Zvi)

Selected Book Chapters etc

"U.S.-Soviet Attempts to Regulate Military Activities in Space", in U.S. Soviet Security Cooperation: Achievements, Failures, Lessons. Alexander George, Phillip Farley, Alexander Dallin, editors. Oxford University Press, 1988. (with Sidney Drell)

"Interactive Learning in US Soviet Arms Control", in Learning in US and Soviet Foreign Policy, George Breslauer and Philip Tetlock, eds., Westview Press, 1991.

"The Superpowers and Regional Conflicts After the Cold War", in Breslauer, Kriesler, and Ward, ed. Regional Conflicts after the Cold War, Institute of International Studies, Berkeley, 1991.

"Does NATO Have A Future?", Beverly Crawford, ed. The Future of European Security, IIS, Berkeley, 1992.

"Security After 1989," in Nuclear Weapons In The Changing World : Perspectives From Europe, Asia, and North America, Patrick Garrity and Steven A. Maarenan eds. New York: Plenum Press, 1992.

"Institutions and Change", in Micheal Doyle and G. John Ikenberry, eds. New Thinking in International Relations, Westview Press, 1997.

"European Union Conditionality", in Barry Eichengreen, Jeffrey Frieden, and Jurgen Von Hagen, eds. Politics and Institutions in an Integrated Europe, Springer-Verlag, Berlin, 1995.

"Counterfactuals Past and Future", in Phillip Tetlock and Aaron Belkin, eds., Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives, Princeton University Press, 1996.

"Nested Institutions and European Monetary Union", in Vinod Aggarwal, ed. Institutional Designs for a Complex World : Bargaining, Linkages, and Nesting Cornell University Press, 1998.

"Why the Changed Relation Between Security and Economics Will Alter the Character of the European Union", (with John Zysman), in Zysman and Andrew Schwartz, eds., Enlarging Europe: The Industrial Foundations of a New Political Reality Berkeley: IAS, 1998.

"A Modest Proposal for NATO Expansion", in Robert W. Rauchhaus (ed.), Explaining NATO Enlargement, London: Frank Cass, 2000. Also in Contemporary Security Policy, Vol.21, No.2 August 2000.

"Governance and Politics of the Internet Economy -- Historical Transformation or Ordinary Politics With a New Vocabulary?" (with John Zysman) in International Encyclopedia of the Social and Behavioral Sciences, Neil Smelser and P. B. Baltes, eds. Oxford: Elsevier, 2000.

"National Security and The War Potential of Nations," in International Encyclopedia of the Social and Behavioral Sciences, Neil Smelser and P. B. Baltes, eds. Oxford: Elsevier, 2000.

"Tools for Thought", in Tracking a Transformation, Brookings Institution, 2001. (with Brad DeLong, John Zysman, and Stephen Cohen).

"The Political Economy of Open Source Software and Why It Matters," in Digital Formations: IT and New Architectures in the Global Realm, Robert Latham and Saskia Sassen, eds. New Jersey: Princeton University Press, 2005.

"Patterns of Governance in Open Source," in Chris DiBona, Danese Cooper, and Mark Stone, eds., Open Sources 2.0, The Continuing Evolution. Sebastopol CA: O'Reilly, 2005.

"From Linux to Lipitor: Pharma and the Coming Reconfiguration of Intellectual Property," in John Zysman and Abraham Newman, eds., How Revolutionary was the Digital Revolution: National Responses, Market Transitions, and Global Technology. Stanford CA: Stanford University Press, 2006.

"Probing the Value of Shared Data in the Modern Economy", Report to the Kaufmann Foundation, 2012 (With AnnaLee Saxenian)

“Deviant Globalization,” (in Michael Miklaucic and Jacqueline Brewer, ed., *Convergence: Illicit Networks and National Security in the Age of Globalization*, National Defense University Press, 2013 (with Nils Gilman and Jesse Goldhammer)

“Why Universities and Foundations Should Get Together Sooner”, *Chronicle of Higher Education* April 2017 (with James Goldgeier, Bruce Jentleson, and Jessica Trisko Darden.)

Selected Recent Policy Writing and Engagement

Inertia is the Enemy of Cybersecurity, *The Hill* 11/6/21 <https://thehill.com/opinion/cybersecurity/580383-inertia-is-the-enemy-of-cybersecurity>

Cyber Workforce Incubator, 2017, <https://cltc.berkeley.edu/wp-content/uploads/2017/04/Cyber-Workforce-Incubator.pdf>

Resilient Governance for Boards of Directors: Considerations for Effective Oversight of Cyber-Risk, 2019. <https://cltc.berkeley.edu/wp-content/uploads/2020/01/Resilient-Governance-for-Boards-of-Directors-Report.pdf>

A Data Sharing Discipline, 2020. https://cltc.berkeley.edu/wp-content/uploads/2020/09/A_Data_Sharing_Discipline.pdf

Digital Insecurity is the New Normal, *New York Times* 5/15/17 <https://www.nytimes.com/2017/05/15/opinion/cyberattacks-digital-insecurity.html>

Reducing the Waste from our Digital Lives, *Noema* April 2021 <https://www.noemamag.com/reducing-the-waste-from-our-digital-lives/>

Website Blocking as a Proxy of Policy Alignment, *First Monday* January 2021 <https://firstmonday.org/ojs/index.php/fm/article/view/11415>

The Art of Communicating Risk, *Harvard Business Review* 9/24/20 <https://hbr.org/2020/09/the-art-of-communicating-risk>

How Might the Sleeper Agents from ‘The Americans’ Interfere in the Election, *Lawfare* 8/4/20 <https://www.lawfareblog.com/how-might-sleeper-agents-americans-interfere-election>

The Long Shadow of the Future, *Noema* June 2020 <https://www.noemamag.com/the-long-shadow-of-the-future/>

Data, Rivalry, and Government Power: Machine Learning is Changing Everything. *Global Asia* March 2019 <https://www.globalasia.org/data/file/articles/f95045850aa30d155ee4d75911d2c7a1.pdf>

China's Long Game in Techno-Nationalism. First Monday 2018 <https://www.firstmonday.org/ojs/index.php/fm/article/view/8085/7209>

It's the Year 2020: How is Your Cybersecurity? US News 5/2/16 <https://www.usnews.com/news/best-countries/articles/2016-05-02/cybersecurity-in-2020-will-the-internet-read-emotion>

**IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

TIKTOK INC.)	
)	
and)	
)	
BYTEDANCE LTD.,)	
)	
<i>Petitioners,</i>)	
)	
v.)	No. 24-1113
)	
)	
MERRICK B. GARLAND, in his)	
official capacity as Attorney General)	
of the United States,)	
)	
<i>Respondent.</i>)	

DECLARATION OF ADAM PRESSER

1. I am TikTok's Head of Operations and Trust & Safety, a role I have served in since March 2024, and I am employed by Petitioner TikTok Inc. Between June 2023 and March 2024, I was TikTok's Head of Operations, and before that, from April 2022 to June 2023, I was Vice President and TikTok Chief of Staff. As Head of Operations and Trust & Safety, my responsibilities include cultivating, maintaining and protecting TikTok's global content ecosystem. The teams I lead manage

our content operations and distribution all over the world, as well as our efforts to identify and remove harmful content on the platform globally. As a senior executive, I have also become broadly familiar with our operations and policies across a range of areas, including TikTok's data privacy and security policies, engineering operations, and our engagement with stakeholders and regulators in the United States and abroad.

2. I am a U.S. citizen born and raised in Los Angeles, California. I have a B.A. and M.A. from Yale University, a J.D. from Harvard Law School, and an MBA from Harvard Business School. Before I joined TikTok, I worked for Warner Bros. Entertainment and then WarnerMedia, most recently as Executive Vice President, International and Head of WarnerMedia China, Australia and New Zealand, and Head of WarnerMedia International Home Entertainment Licensing. I have extensive experience working in multinational business operations in a variety of structures, including with joint ventures, licensing partners, and, as with TikTok, globally integrated businesses.

3. The purpose of this declaration is to provide an overview of the TikTok platform, including how we protect U.S. users' data and guard against foreign government influence. I also explain why the U.S. TikTok platform cannot realistically be severed from the rest of the global platform in one year, as I understand would be required to avoid a ban of TikTok under the "Protecting Americans from Foreign Adversary Controlled Applications Act."

I. Background on Petitioners TikTok Inc. and ByteDance Ltd.

4. Like many global businesses, TikTok operates through multiple corporate entities. In the United States, the TikTok platform is provided by TikTok Inc., a California-incorporated company that has its principal place of business in Culver City, California and offices in New York, San Jose, Chicago, and Miami, among other locations. TikTok Inc. has thousands of employees in the United States. References in my declaration to "TikTok Inc." are to this specific corporate entity; references to "TikTok" are to the online platform.

5. TikTok Inc.'s ultimate parent company is ByteDance Ltd., a Cayman Islands-incorporated equity holding company that has multiple operating subsidiaries, including in China. References in my

declaration to “ByteDance Ltd.” are to this specific corporate entity, whereas more general references to “ByteDance” are to the corporate group, including its operating subsidiaries. ByteDance was founded in 2012 by two Chinese engineers. Today, approximately 58 percent of ByteDance Ltd. is owned by global institutional investors, including General Atlantic and Susquehanna International Group; 21 percent is owned by its global employee workforce; and 21 percent is owned by one of its founders, Zhang Yiming (a Chinese national who lives in Singapore).

6. In addition to TikTok Inc., which provides the TikTok platform in the United States, other subsidiaries of ByteDance Ltd. provide several other applications, services, and online platforms in the United States, including for content sharing, video and music editing (such as the popular video-editing app CapCut), e-commerce, gaming, and enterprise productivity.

II. The TikTok Platform

7. TikTok is an online platform that enables users to create, share, and view videos. TikTok’s mission is “to inspire creativity and

bring joy,”¹ and we seek to bring this mission to life through the products we build, the content we cultivate and recommend, and the rules we publish and enforce to keep harmful content away from our users.

8. TikTok is designed to provide a creative and entertaining forum for our users to express themselves and make connections with other content creators and viewers. TikTok users primarily engage with the platform by creating and sharing videos or by watching and interacting with videos posted by others. In addition to sharing and commenting on videos, users can connect with one another in a variety of other ways, including “tagging” other users in the comments, using the app’s “duet” and “stitch” tools to create new content that incorporates and responds to content created by others, using the “TikTok LIVE” feature to communicate live with others on the platform, and sending direct messages to one another. The TikTok platform is offered in more than 170 countries, but it is not offered in mainland China.

¹ Our Mission, TikTok, https://www.tiktok.com/about?lang_en (last visited June 17, 2024).

9. TikTok is a globally integrated platform, meaning that content posted in one country is generally available to users in any of the 170+ countries in which TikTok is available. There is an enormous array of international content available to U.S. users on the platform, some of which is extremely popular. Just to take a few examples, there is content about global sporting events like the Olympic Games (@olympics has 8.3 million followers), international sports teams (@realmadrid has 45.5 million followers), and international music such as K-pop (one of the most popular groups, BTS, has 65.3 million followers) and Tomorrowland, an annual music festival in Ibiza, Spain (@tomorrowland has 5.7 million followers).

10. TikTok was first launched globally in May 2017 in over 150 countries, including the United States. After ByteDance Ltd. acquired another short-form video platform, musical.ly, and moved its user base to TikTok, TikTok was re-launched in the United States in August 2018.

11. Since then, TikTok has grown to become one of the most widely used online platforms in the world. TikTok has more than 170 million monthly users in the United States and more than 1 billion

users worldwide. With so many U.S. users, the volume of content created and viewed in the United States is correspondingly immense. In 2023, TikTok users in the United States uploaded more than 5.5 billion videos, which were viewed more than 13 trillion times here and abroad; half of those video views came from users outside the United States. In the same year, TikTok users in the United States viewed content from outside the United States more than 2.7 trillion times, which accounted for more than a quarter of all video views in the United States. U.S. content is also disproportionately popular abroad; for example, last year, even in several of TikTok's non-U.S. English-speaking markets, content from the United States comprised more than a third of all video views.

12. TikTok's initial growth was spurred by its appeal to those who value the blend of light entertainment and humor our platform provides. Today, TikTok also has become a forum for all types of speech, including about politics, sports, family, religion, and users' jobs and hobbies.² Many content creators use our platform to express their

² TikTok does not, however, permit paid political advertising on the platform. *See* TikTok Business Help Center, Ad Policy Handbook: North

opinions, share their stories, support their preferred political candidates, and speak out on today's many pressing issues, all to a global audience of more than one billion monthly users.

13. TikTok Inc. itself maintains an active account on TikTok, operated by a U.S.-based team, which has more than 80 million followers globally. TikTok Inc. uses the TikTok platform to create and share its own content about issues and current events, including, for example, its support for small businesses, Earth Day, and literacy and education. The company also interacts with users by promoting public-interest content on TikTok, such as our “EduTok” campaign, which encourages users to create and share educational and motivational content on a variety of themes. The company has also launched other campaigns to promote public interest content. TikTok users also have the ability to use special filters, special effects, and stickers available on the platform to enhance their content and express their views on issues of public interest.

America (last updated June 2024),
<https://ads.tiktok.com/help/article/ad-policy-handbook-north-america>.

14. Although there are other platforms that allow users to post and share content, TikTok differs from these platforms in important respects. For example, unlike other platforms, TikTok does not host written posts (except insofar as a user posts a video or picture showing written text), and it is not as focused on users' interactions with existing friends, family, or co-workers, like some other platforms are.

15. Instead, the TikTok experience is centered on discovering video content primarily through the app's For You feed, which opens a collection of videos curated by TikTok's proprietary recommendation engine based on an individual user's interests and how the user interacts with content they watch. With the For You feed, TikTok's focus is on facilitating users' discovery and exploration of new content and new communities that might be of interest to them. The For You feed provides individual, regular TikTok users a unique ability to discover new content and, for those who choose to post their own content, to reach a new and broader audience. The For You feed (and its recommendation engine) is central to the TikTok experience and one of the defining features of the TikTok platform that made it successful.

16. Although the For You feed is the most popular way users use TikTok, users can explore content on TikTok in a variety of other ways. For example, users can use the search function to find content about particular topics they are interested in. Videos in search results are sorted according to a combination of factors, including relevance to a user's search query and other users' level of engagement with the video. Relevance is determined based on things like video captions, video text, and "hashtags," all of which can only be added by the users themselves upon uploading the videos.

17. On TikTok and other online platforms, hashtags function as content aggregators, which means that a user can locate other content with that hashtag by searching for the hashtag or clicking on the hashtag in a comment or video caption. Hashtags help users to find content that appeals to their particular hobbies, athletic pursuits, or identities and to connect with others, including through #booktok (33.8 million posts), #baseball (4.3 million posts), #blacktiktok (4.7 million posts), and #fitness (37.8 million posts). Many creators also use the platform to post product reviews, business reviews, and travel

information and reviews. For example, #travel has 46.1 million posts on TikTok.

18. Because a significant percentage of videos posted on TikTok do not have any hashtags at all, hashtags will rarely capture all of the content associated with a specific topic. For that reason, the platform's search function is based on a number of inputs, not just hashtags. For example, while #taylorswift is associated with 13.2 million posts on TikTok, a search for the term "Taylor Swift" would generate many more posts. For the same reason, it is not possible to compare the prevalence of different kinds of content on TikTok, or make comparisons to other platforms, by looking only at hashtag numbers. Through our Research Tools, qualifying researchers in the U.S. and Europe can apply to study public data about TikTok content and accounts.

19. Users can also view a feed consisting only of content posted by those creators they have decided to "follow." That allows users to curate their own viewing experience, rather than only relying on TikTok to do so.

20. Creators come to TikTok because of the platform's unique attributes. In my experience, creators join TikTok because of its ability

to facilitate discovery through organic reach—that is, the number of people who see a post through unpaid distribution. TikTok’s organic reach allows creators to reach large numbers of users—beyond their current universe of followers—without any paid promotion. Moreover, TikTok’s recommendation system facilitates users’ access to content created by a wide range of individuals, meaning that it is not unusual for videos created by regular people to “go viral” and receive thousands, if not millions, of views. Many platforms offer creators a forum to reach new audiences. But TikTok is unique in its ability to generate reach for regular people. For example, nine of the top ten TikTok accounts with the most followers were regular people before they joined the platform and started posting, and the tenth account is TikTok’s own account. By comparison, for several of our competitors, the most-followed accounts belong to people who are independently famous, like athletes, actors, and musicians.

III. The Content Available on the TikTok Platform

21. We always strive to show our users content that serves our mission to “inspire creativity and bring joy” in a safe environment. In service of that goal, we use three main editorial processes to determine

what content is shown to users: content moderation, content recommendation, and video promotion and filtering.

A. Content Moderation

22. The first process that determines the content available to users is content moderation. As noted above, I oversee the TikTok Trust & Safety team, which is responsible for content moderation globally. This year, we anticipate spending more than \$2 billion on Trust & Safety globally, and the TikTok Trust & Safety team I oversee includes more than 40,000 employees and contractors worldwide.

23. Consistent with our guiding principle to enable free expression while preventing harm, the goal of content moderation is to create a welcoming and safe experience for our users. The content moderation process applies to all content available on the platform, whether viewed on the For You feed or discovered via searching.

24. Our approach to content moderation is built on the foundation of our Community Guidelines, a publicly available collection of rules and standards that apply to all TikTok users and content.³ The

³ *Community Guidelines*, TikTok (last updated April 17, 2024), <https://www.tiktok.com/community-guidelines?lang=en>.

team that writes the Community Guidelines reports to me, and I ultimately approve the Community Guidelines before they are published on the platform and our website. The Community Guidelines were created and are continually refined in consultation with third-party experts, including our U.S. Content Advisory Council. The Content Advisory Council brings together groups of American independent experts who help us develop forward-looking policies and processes to help create a safe platform for everyone. They work with us to inform and strengthen our policies, product features, and safety processes.

25. The Community Guidelines include rules for what is allowed on TikTok, as well as standards for what content is eligible for recommendation to users in the For You feed. Among other things, the Community Guidelines prohibit nudity; promotion of or incitement to violence; promotion of criminal activities that may harm people, animals, or property; hate speech, hateful ideology, and hateful behaviors; promotion of violent or hateful political organizations; animal abuse; and harassment and bullying. Of course, on a platform as large as ours, it is natural for people to have different opinions, and we

welcome that, but we do not allow influence operations, where networks of accounts work together to mislead people or our systems and try to strategically influence public discussion. The Community Guidelines also outline our policies for dealing with misinformation. And we also have a publicly disclosed policy regarding State-Affiliated Media.

26. We proactively enforce our Community Guidelines through a mix of technology-based and human moderation. Every video uploaded to TikTok goes through automated moderation before it appears on the platform so that content flagged as potentially violative can be automatically removed or escalated for human review by trained moderators. More than 75% of all videos removed for violating the Community Guidelines are never viewed by a single user. We also encourage users to take advantage of various tools provided through the app or on the website to report content that they believe violates the Community Guidelines. If we identify violative content—on our own or through our users—we remove such content from the platform. The team responsible for enforcing the Community Guidelines globally also reports to me. This team is governed by strict company-wide policies intended to ensure that content is moderated in accordance with our

Community Guidelines, and we enforce these policies with measures to track and audit moderation decisions.

27. In total, over 176 million videos were removed from TikTok in the period of October through December 2023 for violating the Community Guidelines. We publicly disclose these and other statistics regarding our enforcement of the Community Guidelines in our quarterly Community Guidelines Enforcement reports, which are posted on our website.⁴ We also publish a report with information about covert influence operations we disrupt, including how they were detected, how many accounts we removed, how many followers the accounts had, and a description of the operations, including where it was operating from and the country that was targeted.⁵ In addition to our transparency reports, as I mentioned above, through our Research Tools, qualifying researchers in the U.S. and Europe can apply to study public data about TikTok content and accounts, which provides additional transparency into the activity on our platform.

⁴ *Community Guidelines Enforcement Report*, TikTok (published Mar. 19, 2024), <https://www.tiktok.com/transparency/en/community-guidelines-enforcement/>.

⁵ *Covert Influence Operations Report*, TikTok, <https://www.tiktok.com/transparency/en/covert-influence-operations/>.

28. Even if content does not violate our Community Guidelines, we take steps as part of our content moderation processes to limit access to content that may not be suitable for certain users. For example, even though it may not violate the Guidelines, content depicting consumption of excessive amounts of alcohol by adults is not eligible for recommendation in the For You feed. Additionally, videos that some users may find to be distressing but that involve a subject of important public interest, are instead covered by “opt-in viewing screens” when flagged. These opt-in screens warn the user that the video may contain sensitive material and give the user the option to either view the content or skip to the next video.⁶ Such videos are also ineligible for recommendation on users’ For You feeds.⁷

B. Content Recommendation

29. The second process we use to determine what content to show to users is content recommendation. Content recommendation is

⁶ Cormac Keenan, Refreshing Our Policies to Support Community Well-Being, TikTok (Dec. 15, 2020), <https://newsroom.tiktok.com/en-us/refreshing-our-policies-to-support-community-well-being>; Tara Wadhwa, New Resources to Support Our Community’s Well-Being, TikTok (Sept. 14, 2021), <https://newsroom.tiktok.com/en-us/new-resources-to-support-well-being>.

⁷ Keenan, *supra* n.6; Wadhwa, *supra* n.6.

implemented by TikTok's recommendation engine, a sorting and ranking mechanism that uses statistical modeling to select videos for a user's For You feed.

30. The recommendation system analyzes various signals from the user and other users, such as their likes, comments, and what they watch. The recommendation engine identifies a pool of candidate videos for a user, then scores and ranks those videos using machine-learning models that seek to determine which video would be most interesting to the user. As I described above, certain content is not eligible for recommendation in the For You feed and this content is not part of the candidate pool. To evaluate whether a user would find a particular video interesting, these models assign different weights to a variety of factors, including user engagement or activity information (such as video playtime, likes, shares, accounts followed, comments, content created), account or device information (such as language preference, country setting, device type), and video information (such as captions, sounds, hashtags). The system may adjust the weight assigned to a particular parameter if it "learns" that it is more or less important than

other factors in determining whether users are, or a particular user is, likely to engage with a given video.

31. In essence, the recommendation engine functions as a large matching system, matching users with content they are predicted to like based on their viewing habits.

32. The source code for TikTok's recommendation engine was originally developed by ByteDance engineers based in China and is continually developed by the TikTok Global Engineering Team. The recommendation engine is customized for TikTok's various global markets, including in the United States, and that customization is subject to special vetting in the United States. In addition to those protections, which I describe below, as with other source code, we have technical measures in place intended to ensure that only employees with appropriate access controls are able to update the recommendation engine, and those updates are also auditable.

C. Video Promotion and Filtering

33. Video promotion and filtering is the third process determining what content is shown to users, and is similarly intended to ensure that users have a positive experience with content they enjoy.

We may promote specific content (e.g., highlights from the Super Bowl, or videos from a Beyoncé concert) in line with company content policies, including to support the inclusion of diverse and high-quality content on the platform.

34. Our internal policies strictly limit which employees can request promotion of content. Each request to promote a video is manually reviewed and either approved or rejected based on an assessment of whether it follows the platform's content policies, including to support content diversity and quality (for example, being engaging and meaningful and focusing on timely/relevant content) and business objectives. Each video that is promoted is reviewed at least once by a human reviewer, and these teams are regionalized, so all videos promoted in the U.S. are reviewed by a U.S.-based reviewer. Our global security teams also audit promotion requests to ensure that they are consistent with our policies. Promotion currently impacts less than 1% of video views in the United States.

35. Just as we promote certain specific content to improve the user experience, we also apply a set of rules to filter out and disperse certain content, i.e., not show one video after another about the same

subject, in users' For You feeds. The objective of filtering content is to make the platform safer and more enjoyable for our users and to support commercial and product goals such as prioritizing content from the same country, avoiding duplication, and ensuring appropriate video length. For example, we filter out from users' For You feed content that is predicted to be low quality (e.g., extremely short videos). We also disperse content to try to ensure sufficient diversity of content in a user's For You feed.

36. We also attempt to identify and disperse content that, viewed sparingly, is not harmful, but viewed repeatedly could be problematic, such as content about exercise, dieting, or mental health. These videos may be eligible for the For You feed, but, to protect our community, we work to interrupt repetitive patterns to ensure they are not viewed too often.

IV. TikTok's Efforts to Safeguard U.S. User Data and the Integrity of the Platform Against Foreign Government Influence.

37. TikTok has undertaken unprecedented efforts to safeguard U.S. user data and protect the integrity of the platform against foreign government influence.

38. Like other platforms, TikTok collects certain information from users in accordance with its Privacy Policy and Terms of Service, to which users must agree as a condition of signing up for the app.⁸ Pursuant to the Privacy Policy, TikTok collects users' usernames, dates of birth, and, depending on how they sign up for the app, a user's phone number or email address.⁹ Notably, however, there are also several categories of data that we do not collect. Unlike other platforms, for example, TikTok does not require its users to provide certain types of personal identifying information, such as the user's real name, employment information, or familial relationships or relationship status. The current version of the TikTok app also does not collect GPS information from U.S. users.

39. Starting in 2019, the U.S. government expressed concerns that the Chinese government could obtain access to user data TikTok collects from U.S. users, or compel ByteDance to manipulate the TikTok

⁸ *Privacy Policy*, TikTok (last updated March 28, 2024), <https://www.tiktok.com/legal/page/us/privacy-policy/en>; *see also Terms of Service*, TikTok (last updated November 2023), <https://www.tiktok.com/legal/page/us/terms-of-service/en>.

⁹ *Privacy Policy*, TikTok (last updated March 28, 2024), <https://www.tiktok.com/legal/page/us/privacy-policy/en>.

platform to promote the Chinese government's agenda in the United States. We disagree that these concerns are well-founded, but made a voluntary decision to engage for several years with the Committee on Foreign Investment in the United States on how to address those concerns. Following extensive engagement and the incorporation of significant U.S. government feedback, that process culminated in a 90-page draft National Security Agreement, the latest draft of which we provided to the government on August 23, 2022.

40. The full range of commitments is described in the draft National Security Agreement, but in summary it contains several layers of protections that would enable the U.S. government to validate the security of U.S. user data and confirm that the platform is free from improper influence by any foreign government. To our knowledge, no other online platform provides these kinds of protections, which even include a “shut-down option” that would give the government the authority to suspend TikTok in the United States if we violate certain obligations under the agreement. These protections are in addition to our existing policy, technical, and transparency safeguards

implemented on a global basis to safeguard TikTok user data and protect the integrity of the platform against foreign interference.

41. Although the draft National Security Agreement was never signed, we have voluntarily begun implementing many measures that do not require the U.S. government's cooperation. We have invested more than \$2 billion on that effort—sometimes referred to as “Project Texas.” Among the steps we have taken as part of this initiative are the following:

42. Independent Governance. We have created a special purpose subsidiary of TikTok Inc. called TikTok U.S. Data Security Inc. (“TikTok USDS”) to control access to protected U.S. user data (as defined in our draft National Security Agreement) and monitor the security of the platform. The TikTok USDS team is currently led by Interim General Manager Andy Bonillo and Interim Security Officer Will Farrell, both of whom are U.S. citizens with significant experience working with the U.S. government on national security and cybersecurity matters. All TikTok USDS employees, of which there are now over 2,000, report to Mr. Bonillo and Mr. Farrell. TikTok USDS

employees work in offices that are physically separate from that of other TikTok or ByteDance personnel.¹⁰

43. Data Protection and Access Controls. We have partnered with Oracle Corporation on the migration of the U.S. platform and protected U.S. user data to Oracle's cloud environment. Every U.S. user now interacts with a version of TikTok that is run in the Oracle environment, and we have taken steps to store protected U.S. user data there. Access to the Oracle environment is limited to only TikTok USDS personnel, unless authorization is given by TikTok USDS pursuant to limited exceptions, such as for legal and compliance purposes.

44. Software Assurance. TikTok USDS and Oracle review updates to the U.S. TikTok app developed by employees outside TikTok USDS, and all software updates are deployed, i.e., implemented on the U.S. TikTok platform, by TikTok USDS personnel. TikTok USDS also reviews changes to the platform code base, and Oracle has full access to

¹⁰ The draft National Security Agreement requires TikTok USDS to be governed by an independent board with Security Directors whose appointment would be subject to the U.S. government's approval and would exclude ByteDance and its subsidiaries and affiliates from any oversight of TikTok USDS. TikTok USDS has provided nominees for these directors to the U.S. government, but the government has not yet approved them.

review the entire source code, including any updates, in dedicated transparency centers located in Columbia, Maryland; Denver, Colorado; the United Kingdom; and Australia.

45. Content Assurance. TikTok's U.S. recommendation engine is stored in the Oracle cloud. TikTok USDS now deploys the recommendation engine in the United States, and as noted above, Oracle has full access to review the entire TikTok platform source code, which includes the algorithm for the recommendation engine. TikTok USDS also reviews and approves content promotion requests to help ensure that content promotion on the U.S. TikTok platform is conducted consistently with our policies and is free of foreign-government interference.

V. The Prohibitions in the Act Will Lead to TikTok Being Inoperable in the United States.

46. As I understand it, the Act contains two types of prohibitions. First, it prohibits “services to distribute, maintain, or update” the TikTok platform in the United States “by means of a marketplace (including an online mobile application store).” Second, it prohibits “internet hosting services to enable the distribution, maintenance, or updating of” the TikTok platform. Together, these

prohibitions would render the TikTok platform inoperable in the United States.

47. With respect to the first prohibition, removing the app from U.S. app stores will halt the influx of any new U.S. users, immediately foreclosing millions of Americans who have not yet downloaded the app from joining TikTok.

48. Even those users and creators who choose to stay on the platform would be affected by the removal of the TikTok app from app stores. We also regularly update the software for the TikTok app, and consumers receive those updates via app store downloads. This prohibition would accordingly prevent users from downloading updates to the app, including security fixes. The inability to download updates would eventually render the app incompatible with the TikTok platform and therefore inoperable.

49. The second prohibition, on the provision of internet hosting services, would likewise prevent us and our commercial partners from providing the services that enable the TikTok platform to function, effectively shutting down TikTok in the United States. For example, internet service providers may stop routing traffic to TikTok.com; data

centers may not renew contracts because it would be unclear if they would be allowed to host TikTok code, content, or data; and content delivery networks (“CDNs”) that are spread throughout the country may also be covered. The termination of these services would cripple the platform in the United States and make it totally unusable.

50. Even a temporary implementation of these prohibitions would cause significant and irreversible harms to our business and our brand. Users and content creators tend to develop lasting brand loyalty when it comes to social media and online entertainment platforms, and if we lose these users and content creators to our competitors, even on a temporary basis, some are not likely to return, even if the prohibitions are later lifted. Accordingly, even if the prohibitions of the Act are later lifted, we would not be able to make up for lost ground, because people who would have downloaded TikTok will have already turned to other competing platforms.

51. The prohibitions also would dramatically undercut the commercial goodwill associated with TikTok and impede our ability to form and maintain commercial partnerships. By destroying the vibrant TikTok community in the U.S., the prohibitions will deal a heavy blow

to our reputation and attractiveness as a commercial partner. This collapse of goodwill will harm our revenues from existing partnerships and prevent us from realizing revenue from future opportunities, as prospective partners forge relationships with our competitors instead. If we are perceived to be an unreliable partner in the marketplace, advertisers will build partnerships with other platforms.

52. Being banned from the United States will also devastate our U.S. workforce, permanently harming our ability to recruit and retain talent. TikTok is a technology company, and we compete fiercely for the software engineers and other talent we rely upon to run our business. These candidates often have multiple offers from other companies. Since the Act was signed into law, our competitors have been aggressively trying to recruit our talent. As the prohibitions come into effect, these problems with recruitment and retention will be greatly magnified, given that the business these employees support would be banned in the United States.

VI. Severing the U.S. TikTok Platform from ByteDance and the Global TikTok Platform.

53. I understand that the only way to avoid those prohibitions is if the U.S. TikTok platform is sold, leaving no subsequent operational

relationship with the rest of the global TikTok platform or the ByteDance affiliate employees that currently support it.

54. As discussed above, TikTok in the United States is an integrated part of the global TikTok platform. The global TikTok business is led by a leadership team based in Singapore and the United States. Many of the teams that support the global TikTok platform, including engineering, operations, Trust & Safety, and advertising sales, are spread across several different corporate entities and countries.

55. Because the platform and the content is global, the teams working on the platform, and the tools they use, necessarily must be, as well. For example, as I mentioned above, we do not allow animal abuse on the platform, and we use software tools to identify content depicting animal abuse. It is important that the tools used to automatically detect animal abuse are effective and consistent. We have accordingly developed and refined those tools at the global level, drawing on resources from multiple functions in different countries.

56. As another example, several members of my senior leadership team are based outside the United States, including in

London, Dublin, and Singapore, and they are responsible for a wide range of global functions on our Operations and Trust & Safety teams, including managing all content moderators globally, overseeing global publisher relationships, working with law enforcement authorities around the world to prevent crimes on the platform, and managing copyright takedown requests.

57. The global TikTok platform also relies on the support of employees of other ByteDance subsidiaries for some functions, including the development of portions of the computer code that runs the TikTok platform. These integrated relationships are consistent with our commitments under Project Texas, pursuant to which TikTok USDS and Oracle vet updates to the U.S. platform developed by engineers outside TikTok USDS. In other words, Project Texas contemplates that source code supporting the TikTok platform, including the recommendation engine, will continue to be developed and maintained by ByteDance subsidiary employees, including in the United States and in China, and that any such source code is reviewed and vetted by TikTok USDS and Oracle.

58. Given these integrated relationships, there are several reasons why a severance of the U.S. TikTok platform from the rest of the globally integrated TikTok platform and business is not feasible.

59. First, as I have mentioned, TikTok is a globally integrated online platform where content created in one place is generally available everywhere else. The same is true of TikTok's competitors in the United States, like YouTube, Instagram, and Snapchat. For example, as mentioned above, in 2023, half of views of videos posted in the United States came from users outside the United States, and non-U.S. content accounted for more than a quarter of all video views in the United States.

60. Divesting the U.S. TikTok business in a way that precludes any further operational relationship with the rest of TikTok outside the United States would prevent international content from being seamlessly available in the U.S. market and vice versa. I understand that, to avoid a ban, the Act requires divestment of the U.S. TikTok application, without any ongoing operational relationship with non-U.S. TikTok or ByteDance entities, including any agreement to share user data. In the absence of an operational relationship, including an

agreement to share content and data with the entities that operate the global platform, the U.S. TikTok platform would become an “island” where Americans would have an experience isolated from the rest of the global platform. U.S. users on a U.S.-only version of TikTok would be unable to access the content posted by any non-U.S. TikTok users, and U.S. creators would be unable to reach that audience abroad.

61. Such a U.S.-only version of TikTok would be unable to compete with rival, global platforms. The rich pool of global content on the TikTok platform helps generate more users and more traffic, which in turn attracts more (and more popular) creators, which in turn attracts more user traffic, restarting the cycle. Our ability to attract advertisers and drive revenue depends on user engagement. A platform of exclusively American users will be significantly less attractive to global advertisers and creators than a rival platform operating on a global scale, leading to the reverse of the cycle I described above.

62. The operational costs associated with running an online platform for user-generated content, including the extensive Trust & Safety and content assurance operations I have described above, could not be sustained by a purely U.S.-only platform. For example, I

mentioned above that we will spend over \$2 billion on Trust & Safety this year. A U.S.-only platform would likely incur many of the same expenses, including on technology tools and third-party safety experts, because those costs are largely independent of the number of users on the platform and instead are mainly fixed costs associated with continually refining and maintaining a complicated set of technological and human systems and processes for a large platform hosting user-generated content. But while the costs for a U.S.-only platform would be on the same scale as they are currently, the base of revenue to support them would be considerably smaller.

63. Second, setting aside these commercial dynamics, divesting the U.S. TikTok platform in the manner and on the timeline required by the Act would not be technologically feasible because it would require the U.S. platform to be severed from the ByteDance engineers responsible for maintaining and updating its code base.

64. The code base supporting the TikTok platform includes billions of lines of code that have been developed over multiple years by a team of thousands of global engineers, including in China. To complete a divestiture required by the Act, *none* of those thousands of

ByteDance employees would be permitted to continue to support TikTok in the United States. Under those circumstances, there is no question that it would take at least several years for an entirely new set of engineers to gain sufficient familiarity with the source code to perform the ongoing, necessary maintenance and development activities for the platform. Even then, such a newly-created team of engineers would need access to custom-made ByteDance software tools, which the Act prohibits.

65. As I mentioned above, during my time at WarnerMedia and most recently at TikTok, I have worked to implement a variety of corporate relationships and reorganizations, including licensing agreements, joint ventures, mergers, and spin-offs. The divestiture contemplated by the Act is fundamentally different—a sale within one year without any possibility of follow-on cooperation. Such a transaction for a platform of TikTok’s size and scope is infeasible along the timeline dictated by the Act.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury
that the foregoing is true and correct to the best of my knowledge.

Executed this day June 17, 2024.


Adam Presser

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system on June 20, 2024.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

June 20, 2024

/s/ Alexander A. Berengaut
Alexander A. Berengaut
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-600
aberengaut@cov.com

*Counsel for Petitioners TikTok Inc.
and ByteDance Ltd.*